UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIA Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO
Maestría en Ciencias de la Computación

# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UN SISTEMA DE INFORMACIÓN

## (Caso de estudio: Sistema Administrativo Integrado SAI en la Red de datos de la UNEXPO- Puerto Ordaz)

BARQUISIMETO, ENERO 2008

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIA Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO
Maestría en Ciencias de la Computación

# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UN SISTEMA DE INFORMACIÓN

## (Caso de estudio: Sistema Administrativo Integrado SAI en la Red de datos de la UNEXPO- Puerto Ordaz)

Trabajo de Grado presentado como requisito parcial para optar al grado de Magíster Scientiarum en Ciencias de la Computación

**AUTOR:** MSc TERSEK R. YANEISY S.

**TUTOR:** MSc. CLEMANT GLENNYS

BARQUISIMETO, ENERO 2008

## DEDICATORIA

A Dios Todopoderoso, por guiar mis pasos y brindarme salud y sabiduría para lograr culminar esta meta.

A mis padres: Tone Tersek y Dominga Rodríguez de Tersek, por todo el apoyo que siempre me han brindado y por ese amor que es mi fuerza para enfrentar las adversidades.

A mi gran amor, Orlando Escalona por su apoyo incondicional, comprensión e infinita paciencia.

A mis hijos Pedro Luís y José Antonio para que este esfuerzo sirva de ejemplo de superación.

A mis hermanas Yraida e Irlenys quienes siempre me han impulsado al logro de mis metas.

Para ustedes este logro.

Yaneisy

## AGRADECIMIENTO

A la Universidad Centro Occidental “Lisandro Alvarado” (UCLA) por ser mi Alma Mater, donde adquirí valiosos conocimientos, que servirán de mucho en el desempeño laboral.

A la MSc Glennys Clemant, por su orientación y dedicación para desarrollar y llegar a feliz término la investigación.

A la Rectora de la Universidad Nacional Experimental Politécnica Antonio José de Sucre (UNEXPO), Prof. Rita Àñez, por su apoyo y colaboración incondicional para llevar a cabo la presente investigación.

A las autoridades del Vicerrectorado de Puerto Ordaz Prof. Rafael Marcano, Dr. Ovidio León, Prof. Miguel Leyton por brindarme su colaboración en el desarrollo del trabajo de grado.

A mis amigos Dra. Elizabeth Lezama y MSc. Manuel Mújica, por sus valiosos y oportunos consejos.

A todos mis sinceros agradecimientos.

## INDICE GENERAL

## LISTA DE CUADROS

## LISTA DE GRÁFICOS

## LISTA DE FIGURAS

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIA Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO
Ciencias de la Computación

# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UN SISTEMA DE INFORMACIÓN

## (Caso de estudio: Sistema Administrativo Integrado SAI en la Red de datos de la UNEXPO- Puerto Ordaz)

**Autora:** Yaneisy Tersek Rodríguez
**Tutora:** Glennys Clemant

## RESUMEN

La presente investigación tuvo como objetivo principal, establecer un sistema de gestión de seguridad de la información para un sistema de información tomando como caso de estudio el Sistema Administrativo Integrado (SAI) en producción en la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Vicerrectorado de Puerto Ordaz. La misma, se desarrolló bajo la modalidad de estudios de proyecto apoyado tanto en una investigación de campo como en la investigación monográfica documental que permitió la elaboración y desarrollo de una propuesta de un modelo operativo viable para solventar los problemas de seguridad de la información en la Unexpo- Vicerrectorado de Puerto Ordaz. La metodología utilizada se sustentó en tres fases fundamentales, la primera el estudio diagnóstico, la segunda la factibilidad; y la última el diseño del sistema de gestión de seguridad de la Información, tomando como referencia la Norma ISO 27001:2005 y usando una combinación de metodologías y herramientas para la evaluación de los riesgos que ayude a la toma de decisión sobre las opciones de tratamiento de riesgo adecuado. Entre las recomendaciones se destaca la instauración de un plan de gestión de la continuidad del negocio para ayudar a la recuperación y restablecimiento de los procesos interrumpidos en un tiempo prudencial.

**Descriptores**: Sistema de Gestión de Seguridad de la Información SGSI, Seguridad de la información, Sistemas de Información, Redes de Computadoras, ISO/IEC 27001:2005.

# INTRODUCCIÓN

Los violentos cambios tecnológicos que actualmente vive la sociedad y que involucra las telecomunicaciones y la informática han proporcionado claras mejoras pero también nuevos problemas y retos a los investigadores de las Tecnologías de Información y Comunicaciones (TICs). En este mismo orden de ideas, muchas entidades (Bancos, Compañías de Seguros, Administración Pública, entre otros.) almacenan en las bases de datos información corporativa y personal cuyo acceso o difusión a personas o entes no autorizados podría perjudicar gravemente a la empresa o a la(s) persona(s) involucrada(s).

Para la mejor comprensión de un Sistema de Gestión de Seguridad de la Información (SGSI), es importante, en primer lugar, definir el concepto de seguridad, el cual en el diccionario de la Real Academia Española (2006), lo señala como "...estado de seguro; garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo...". De allí, que si se aplica el concepto anterior a la noción de seguridad de la información, debe ampliarse señalando que es una característica de cualquier sistema, libre de peligro, daño o riesgo. Entendiéndose en este trabajo, como peligro o daño a la fuga de información, alteración o la no disponibilidad de la misma en el momento que sea requerida.

Es de destacar que, las organizaciones hoy en día, con la sofisticación tecnológica y la complejidad en el manejo de información, enfrentan distintas amenazas que muchas veces explotan sus vulnerabilidades. El riesgo está siempre presente. El problema es muy serio, en este nuevo siglo, cuando la gestión del conocimiento es una característica vital en las organizaciones, se deben tener formas de minimizar el riesgo de que la información no cumpla con los requerimientos fundamentales de confidencialidad, integridad y disponibilidad.

Es oportuno mencionar, a autores como Albert y Dorofee (2003), quienes sostienen que "Casi el 80% de los valores intelectuales de las corporaciones son

electrónicos, y un competidor puede subir hasta las nubes si roba secretos comerciales y lista de clientes". Este escenario descrito es algo que se presenta regularmente, muchas veces la información deja de ser confidencial y cae en manos de personas no autorizadas, y en la mayoría de los casos causan daños y pérdidas a la empresa. De hecho, la ingeniería social no tiene fronteras para obtener la información que por lo general, se considera confidencial.

Pero el problema es aún más serio, ¿Qué hacen las empresas para asegurar la continuidad ante el impacto de un desastre?, por ejemplo, ¿Qué le pasaría a una empresa financiera, si su servidor queda fuera de servicio?¿Que pasaría si la base de datos de la empresa se pierde? En fin, son escenarios de amenazas que en cualquier momento se pueden poner de manifiesto y hacer colapsar a cualquier empresa, si no se tiene una estrategia de continuidad claramente definida por cada escenario de amenazas previamente identificado, y un plan de reanudación de operaciones que permita operacionalizar rápidamente la estrategia de continuidad del negocio, sin que la empresa colapse financiera y operacionalmente.

De lo anteriormente expuesto, las organizaciones, que desean proteger la información lo primero que deben hacer es identificar los activos de información que tienen impacto en el negocio; luego hacerles un análisis y evaluación del riesgo, y por último, decidir cuales son las opciones de tratamiento del riesgo a implantar a fin de minimizar las posibilidades que las amenazas puedan causar daño a la organización. Los pasos descritos son las acciones que un SGSI busca instaurar en una empresa, como señala Peltier (2001), quien lo define como la preservación de la confidencialidad, integridad y disponibilidad de la información. Igualmente, el modelo ISO 27001:2005, define a un SGSI como "la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información".

De allí, que la presente investigación tiene como objetivo el establecimiento de un Sistema de Gestión de Seguridad de la Información para

un Sistema de información, tomando como caso de estudio el Sistema Administrativo Integrado SAI, en producción en la Universidad Nacional Experimental Politécnica “Antonio José de Sucre”, Vicerrectorado de Puerto Ordaz, con la finalidad de reducir los riesgos de los activos de información que tienen impacto en la misma, mediante controles tomando como referencia la norma ISO 27001:2005, la naturaleza de este estudio se basó en la modalidad de estudios de proyecto apoyado tanto en una investigación de campo como en la investigación monográfica documental.

Asimismo, el trabajo se estructuró en cinco (5) capítulos: el Capítulo I, conformado por el problema, en el cual se desarrolló el planteamiento del problema, objetivos de la investigación, justificación e importancia, alcance y limitaciones del objeto de estudio. Capítulo II, denominado Marco Teórico, contentivo de los antecedentes de investigación, bases teóricas, bases legales y sistema de variables. Capítulo III, Marco Metodológico, contiene la naturaleza y diseño de la investigación con la descripción de las fases del proyecto. Capítulo IV, Propuesta del Estudio, el cual muestra la justificación, objetivos y descripción de la propuesta. Capítulo V, se exponen las conclusiones y recomendaciones de la investigación. Finalmente, se presentan las referencias bibliográficas y los anexos correspondientes.

# CAPITULO I

# EL PROBLEMA

## Planteamiento del Problema

Durante el siglo XX y lo que va del siglo XXI a nivel mundial se han desarrollado importantes cambios en el ámbito tecnológico, económico, social y cultural, entre otros. La complejidad y globalización de los mercados han generado una serie de necesidades de carácter técnico en las grandes empresas obligando a romper con las viejas tradiciones de computadores monousuarios para unirse a una red de ideas globales, donde resalta la accesibilidad de la información y las facilidades de comunicación.

A finales del siglo pasado, la información se convirtió en el recurso más valioso con el que cuentan las empresas, por lo que la seguridad de la información en las redes aparece como un problema potencial de grandes proporciones, originado por la vulnerabilidad a la que se encuentra expuesta la información dentro de los entornos de las redes en Internet e Intranets. Igualmente, las organizaciones tales como: entidades bancarias, compañías de seguros, administración pública, entre otras, contienen en sus bases de datos información corporativa y personal cuyo acceso o difusión a personas o entes no autorizados podría perjudicar gravemente a la empresa o a la(s) persona(s) involucrada(s).

En este sentido, Hernández, E. (2003) señala que se pueden diferenciar dos aspectos muy importantes: *seguridad*, que la información depositada no se pierda o sea alterada de forma incorrecta y *privacidad*, que esta información sólo sea accesible cuando sea necesaria o con los autorizaciones pertinentes.

Como reflejo de la importancia de la seguridad, Hernández, E. (ob. cit), presentó unas conclusiones de un informe realizado por la FBI de Mayo 1999 en la que se estudiaron 521 compañías de distinto tamaño y actividad, donde el 61% presentó pérdidas de información debido al uso no autorizado de sus sistemas informáticos, el 50% de las compañías informaron del abuso en el uso de la red y la media de pérdida por robo o sabotaje fue de 1.1 Millones de dólares.

Es de destacar, que hoy en día, una violación a la seguridad de una red cableada o inalámbrica puede desatar el caos en las operaciones más importantes de una empresa, afectando la productividad, poniendo en peligro la integridad y confidencialidad de los datos y en consecuencia originar desconfianza en los clientes. La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las empresas hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos.

De allí, que en los últimos años, ha sido cada vez más evidente la necesidad de un marco referencial para la seguridad y el control de tecnología de información (TI). Las organizaciones exitosas requieren una apreciación y un entendimiento básico de los riesgos y limitaciones de TI a todos los niveles dentro de la empresa con el fin de llevar una dirección efectiva y controles adecuados. Por eso, el estándar internacional ISO/IEC 27001:2005 adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el sistema de gerencia de la seguridad de la información (SGSI) en una organización.

En este sentido, es responsabilidad de la gerencia decidir cuál es la inversión razonable en seguridad y en control en TI, y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible, ya que la seguridad y los controles en los sistemas de información que ayudan a manejar los riesgos, no los eliminan.

Adicionalmente, el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre.

Es por ello, que en Venezuela las empresas se han abocado a la implementación de Sistemas de Gestión de Seguridad en la Información para lograr la optimización de los servicios y de los sistemas de información. En esta misma línea se encuentra la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", (Unexpo) Vicerrectorado de Puerto Ordaz, Estado Bolívar.

Es de hacer notar, que la Unexpo es la institución politécnica más importante del país y tuvo su origen en el año 1979, cuando de conformidad con el Artículo 10 de la Ley de Universidades, los tres politécnicos: Escuela Técnica Industrial de los Chaguaramos, el Instituto Politécnico de Barquisimeto y el Instituto Universitario Politécnico de Guayana se unificaron mediante Decreto Ejecutivo No. 3087, para formar la hoy Universidad Nacional Experimental Politécnica "Antonio José de Sucre" UNEXPO. Esa integración se traduce en la consolidación de tres sedes: Vicerrectorado Barquisimeto, Vicerrectorado Puerto Ordaz y Vicerrectorado "Luís Caballero Mejías" teniendo como objetivo la formación de profesionales e investigadores creativos, con pensamiento crítico y conciencia ciudadana, para generar, aplicar y difundir el conocimiento, a fin de promover el desarrollo integral del país.

El área tecnológica de la Unexpo es dirigida por la Oficina Central de Tecnología y Servicios de Información (OCTSI), ubicada en Barquisimeto cuyo objetivo es planificar, organizar, dirigir y controlar las políticas emanadas de la alta gerencia, a fin de garantizar la actualización tecnológica, las comunicaciones y los servicios de información requeridos por la institución, fue creada el 04 de mayo del 2005 en sesión extraordinaria del Consejo Universitario Nº 2005-E09-05, en concordancia con los lineamientos de Tecnología y Servicios de Información, aprobado el 20 de julio del 2004 según resolución de Consejo Universitario No. 2004-E14-06. De la estructura organizativa de la OCTSI (ver anexo A), se observa que en cada vicerrectorado

existen las Oficinas Regionales de Tecnología y Servicios de Información ORTSI, conformadas por el Comité de Control de Cambios Regional, las Coordinaciones de Producción y Operaciones (CPO), y Atención a Usuarios (CAU), (ver anexo B).

En esta estructura, la Coordinación de Producción y Operaciones (CPO) es la encargada de mantener la operatividad y funcionalidad de toda la infraestructura tecnológica y de servicios de información que dan soportes a la gestión académica y administrativa del Vicerrectorado de Puerto Ordaz y está conformada por los siguientes grupos de trabajo: Soporte Ambiente Operativo (SAO), Soporte Servicios de Información (SSI) y Soporte Mantenimiento de Seguridad (SMS). Este último grupo de trabajo es el área donde se desarrollará la investigación ya que es la definida estructuralmente para aplicar todo lo referente a seguridad.

Es importante resaltar que la Unexpo, Vicerrectorado de Puerto Ordaz tiene en los actuales momentos la necesidad del fortalecimiento de la seguridad para los sistemas de información en producción, en especial el Sistema Administrativo Integrado SAI, ya que, después del sistema de control de estudio, es el sistema de información más importante, el cual controla toda la parte administrativa.

El Sistema Administrativo Integrado SAI es un servicio de información administrativo que permite integrar los flujos de información de cada una de las unidades administrativas del Rectorado y los Vicerrectorados regionales (Centros de Gastos) de la Unexpo para facilitar la gestión financiera, administrativa, recursos humanos, obras, ingresos, recaudación y contratos, de cada uno de los procedimientos ejecutados por las unidades administrativas, así como también, crear las bases para integrar los flujos de información internos y externos de la institución, conjuntamente con el medio ambiente donde se desarrollan las diferentes actividades.

Al respecto, se ha comprobado por observación directa de la investigadora que la información crítica de los sistemas de información de la

universidad están fácilmente en peligro debido a: fallos en la red, caídas eléctricas, errores de hardware y software, computadores y sistemas informáticos amenazados por virus, hackers, spyware y spam, no existe acciones oportunas que evite la pérdida o eliminación involuntaria de información institucional en los computadores de los usuarios administrativos, usuarios que comparten las contraseñas para ingresar a los sistemas de información, instalación de aplicaciones informáticas sin autorización, no existe un control de acceso a las áreas criticas, entre otros.

Por lo antes expuesto, se determinó que la problemática objeto de estudio es ocasionado por falta de una gerencia proactiva en el área de seguridad con una metododologia que permita detectar las vulnerabilidades y estimar la probabilidad de que ocurran ciertos eventos a fin de minimizar los riesgos en los sistemas y una actitud holística de protección de la información de los usuarios del SAI

De lo anteriormente planteado, se evidencia la necesidad de establecer un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2005, que permita aplicar controles, tales como: política de seguridad, organización de la seguridad de la información, gestión de activos, seguridad de recursos humanos, seguridad física y Ambiental, gestión de comunicaciones y operaciones, control de Accesos, adquisición, desarrollo y mantenimiento de sistemas de información, gestión de incidente de seguridad de la información, gestión de continuidad del negocio y cumplimiento (legales, de estándares, técnicas y auditorias), todo esto con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información manejada en el sistema de información (SAI).

El estudio planteado analizó y dio respuestas a las siguientes interrogantes: ¿Cómo está actualmente la seguridad de la información, en la Universidad Nacional Experimental Politécnica “Antonio José de Sucre”, Vicerrectorado de Puerto Ordaz? ¿Cuál es factibilidad operativa, técnica y económica de diseñar un sistema de gestión de seguridad de la información para

un sistema de información? ¿Qué características debe tener un sistema de gestión de seguridad de la información para el Sistema Administrativo Integrado?

Las respuestas a estas interrogantes permitieron establecer un Sistema de Gestión de seguridad de la información para el Sistema Administrativo Integrado SAI, en producción en la red de datos de la Unexpo Vicerrectorado de Puerto Ordaz.

## Objetivos de la Investigación

### *Objetivo General*

Establecer un Sistema de Gestión de Seguridad de la Información para un Sistema de Información, basado en el estándar internacional ISO/IEC 27001:2005, tomando como caso de estudio el Sistema Administrativo Integrado (SAI) en la red de datos de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Vicerrectorado de Puerto Ordaz.

### *Objetivos Específicos*

1. Diagnosticar la necesidad de un Sistema de Gestión de Seguridad de la Información para los sistemas de información en la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Vicerrectorado de Puerto Ordaz.
2. Determinar la factibilidad operativa, técnica y económica para el establecimiento de un Sistema de Gestión de seguridad de la información en la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Vicerrectorado de Puerto Ordaz.
3. Diseñar un Sistema de Gestión de Seguridad de la Información para el Sistema Administrativo Integrado SAI en la red de datos de la Universidad

Nacional Experimental Politécnica “Antonio José de Sucre”, Vicerrectorado de Puerto Ordaz.

## Justificación e Importancia

En la actualidad las organizaciones y los sistemas de información se enfrentan cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en la informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o negación de servicios son cada vez más comunes, atrevidos y sofisticados.

Es por ello, que los administradores de redes de computadores tienen la misión de evitar que la información que viaja a través de las redes sea capturada, generada o alterada por terceros. En este sentido, la seguridad de la información, protege la información de una amplia gama de amenazas, tanto de orden fortuito como de orden deliberado, garantizando la confidencialidad, integridad y disponibilidad de la misma. De allí que establecer un sistema de gestión de seguridad de la información es el primer paso para aumentar la seguridad.

En este sentido, todas las organizaciones en especial las universidades públicas como organizaciones de servicios deben tomar consciencia e incorporarse dentro de las normas y estándares que involucren seguridad en la información y las leyes venezolanas las cuales brindan un marco legal donde la información tiene un papel preponderante y su tratamiento en lo relacionado a seguridad repercute sobre las responsabilidades de los que administran la tecnologías y servicios de de Información.

Es por ello, que la Universidad Nacional Experimental Politécnica “Antonio José de Sucre” Vicerrectorado de Puerto Ordaz, como universidad pública se encuentra interesada en brindar seguridad a la data crítica e institucional de los sistemas de información en producción en la red de datos.

De allí, la necesidad de establecer un Sistema de Gestión de Seguridad de la Información para el Sistema Administrativo Integrado SAI, basado en la norma ISO/IEC 27001:2005.

La investigación propuesta se justifica técnicamente, ya que se usan metodologías, herramientas y un enfoque sistemático para el análisis y evaluación del riesgo del Sistema Administrativo Integrado SAI, proporcionando una solución efectiva a los problemas de seguridad de la información, basado en la norma ISO/IEC-27001:2005.

Igualmente, el presente proyecto aporta al área de seguridad de información una guía metodológica para la gestión de riesgos en seguridad de información, un campo que no ha sido ampliamente desarrollado. Además, se espera que la investigación sirva como base para futuras investigaciones en el área.

## Alcances y Limitaciones

El presente estudio se realizó en la red de datos de la Universidad Nacional Experimental Politécnica “Antonio José de Sucre”, Vicerrectorado de Puerto Ordaz, en donde se pretende establecer un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2005 para los sistemas de información tomando como caso de estudio el Sistema Administrativo Integrado SAI, y sólo para los módulos de: Presupuesto, Compra, Contabilidad, Almacén y Tesorería, con la finalidad de proponer una solución a la problemática existente descrita con anterioridad.

En cuanto a las limitaciones es importante tomar en cuenta que los aspectos que conforman la confidencialidad de la información son un factor preponderante en el desarrollo de la investigación y es por ello que la información mostrada de la institución es referencial y solo para los efectos académicos respectivos.

# CAPITULO II

# MARCO TEÓRICO

## Antecedentes de la Investigación

Para muchas organizaciones, la información y la tecnología que la soporta, representan uno de los activos más valiosos de la empresa. Es más, en el competitivo y cambiante ambiente actual, la alta gerencia ha incrementado sus expectativas relacionadas con la seguridad de la información y la tecnología que utiliza. Por lo tanto, la gestión requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo debido a que la información contenida dentro de los sistemas informáticos es vital y por lo tanto tiene que ser protegida.

En el presente capítulo se citan investigaciones que han contribuido a generar antecedentes para diseñar un Sistema de Gestión de Seguridad de la Información. Entre los trabajos presentados se destacan los siguientes:

Navarro, A. (2007), presentó el trabajo titulado *Metodología para la Gestión de Seguridad de Información en Venezuela*, cuyo objetivo general es analizar las principales metodologías formales relacionadas con la gestión de la seguridad de información con el propósito de estructurar una que sirva de modelo referencial para su implantación en el mercado venezolano.

Asimismo, el presente trabajo de investigación aporta al área de seguridad de información una guía metodológica para la gestión de riesgos en seguridad de información, un campo que no ha sido ampliamente desarrollado, en donde

existen diversas normativas y metodologías pero no existe una que permita enlazarlas de manera coherente.

El estudio guarda una fuerte relación con la investigación debido a los marcos referenciales estudiados, ISO/IEC 17799, COBIT, (Control Objectives for Information and related Technology), GMITS (Directrices para la gestión de la seguridad, Guidelines for Management of IT Systems) y el CC (Criterios comunes, Common Criteria, CC-ISO 15408), los cuales son marcos bien estructurados, madurados y basados en principios básicos de seguridad, en donde el autor concluyó que estos marcos no son completamente integrables, más bien cada uno puede ser utilizado bajo situaciones específicas. El CC permite evaluar productos y sistemas de seguridad, sirviendo de base para diseño de soluciones de seguridad. GMITS es un marco referencial con un enfoque más administrativo, que resulta más efectivo cuando es implementado en conjunto con un estándar como el ISO/IEC 17799 y complementado con el COBIT, dependiendo del alcance y las necesidades de la organización.

Moulton, B (2004). En Estados Unidos, publicó un artículo titulado *Administración de la TI y seguridad de la información*, señala que la adopción de marcos ampliamente aceptados de control interno, control informático o control de la seguridad de la información puede otorgar credibilidad a los procesos, tecnologías y controles que son necesarios para el soporte de ambientes de seguridad de la información. En la actualidad, marcos tales como COSO (Comité de Organizaciones Auspiciantes), COBIT (Control Objectives for Information and related Technology), ITIL (Information Technology Infrastructure Library) e ISO 17799 son amplios y gozan de aceptación general.

Entre las conclusiones el autor destacan: a) las empresas que disponen de un sistema de administración de la TI superior obtienen un beneficio del 25% más alto que las empresas que poseen un programa de administración insuficiente para los mismos objetivos estratégicos. b) Las empresas que poseen un programa de administración superior a la media presentan una recuperación de sus activos que en media llega a doblar la recuperación de las empresas con

peores sistemas de administración y c) Instituciones financieras, que tienen que cumplir con las leyes y normas de seguridad existentes y nuevas, harían bien en considerar la posibilidad de mejorar sus esfuerzos en la administración de la TI mediante la inclusión de controles de seguridad de la información en la estrategia de administración y mediante la promoción de una cultura del control operacional.

La relación que guarda con el presente estudio consiste en el énfasis que hace el autor de los beneficios que trae para las organizaciones el contar con un sistema de gestión de seguridad de la información.

Córdova, G. (2004). Presentó el trabajo en la Universidad Diego Portales, Santiago de Chile, titulado "*Estudio y comparación de las metodologías ISMS-CMMI"*, realizado en base a las dos metodologías o estándares internacionales que norman la seguridad en las redes y la calidad del software, respectivamente. El propósito del estudio es comprender que tienen en común estos dos estándares internacionales para poder aplicar una metodología de gestión integral hacia una organización que requiera la asesoría en ambos sentidos.

En las conclusiones del estudio el autor señala algunos beneficios de establecer y mantener estándares de calidad, como son: Aumento de la seguridad efectiva de los sistemas de información que garantiza la continuidad del negocio y crea un escudo capaz de responder a las nuevas exigencias del mercado y de los mal intencionados. Mejoras continuas que se producen a través del proceso de auditoria interna. Genera un producto confiable de manera que como un efecto recursivo se incrementa los niveles de confianza de los clientes y socios. Estos estándares de calidad (Modelo Integrado de Mejoras de Capacidad y Madurez, CMMI) y de seguridad (Sistema de Gestión de Seguridad de Información, ISMS) establecen metodologías estandarizadas y algunas certificadas para asegurar la continuidad de los procesos y respaldar su autenticidad. Por último toman un sentido de responsabilidad social empresarial que cada vez es un tema más relevante.

El estudio se relaciona con la investigación debido a que postulan dos metodologías una cualitativa y la otra cuantitativa para proteger la información creada manipulada y procesada al interior de la organización. Igualmente, hace un análisis del la norma ISO 17799 y BS7799-2:2002.

Hamana, J. (2003) realizó un trabajo de grado titulado "*Elementos básicos para modelos de seguridad en organizaciones venezolanas*", utilizando como metodología un estudio de tipo descriptivo no experimental para realizar un análisis conceptual sobre seguridad, las amenazas y las herramientas con las que se cuenta. De igual manera, enumera los puntos necesarios para desarrollar un modelo base para la seguridad de las redes en una organización. Del análisis comparativo de la teoría, se logró extraer elementos indispensables en la comprensión y desarrollo de modelos bases de seguridad para las organizaciones, que sirven como punto de apoyo para la implantación de modelos propios, donde la parte técnica se encarga de evaluar y poner en funcionamiento todo el equipamiento y logística, para cumplir con los lineamientos de seguridad que son planteados desde la alta gerencia, acorde con la visión del negocio. Dentro de las conclusiones obtenidas resalta que el primer paso a seguir por una empresa para ser segura es identificar los puntos débiles de su red, así como también la realización de estudios detallados de puntos de entrada y análisis de protocolos de aplicaciones y a partir de los resultados, se procede a evaluar qué áreas requieren mayor trabajo para garantizar que no serán vulneradas por eventuales atacantes.

El modelo de seguridad de organización propuesto por Hamana, presenta una referencia a seguir en la exhaustiva revisión bibliográfica de esta investigación, como elemento que ayude a vislumbrar la situación de las empresas en Venezuela en lo que concierne a la seguridad informática.

Revilla, C. y Toubes, L. (2003), en su trabajo de grado titulado "*Evaluación e implantación de un sistema de detección de intrusos para la red académica de la Universidad Católica Andrés Bello*", tuvo como objetivo general la implantación de un Sistema de Detección de Intrusos (IDS) en la red

de datos de la Universidad Católica Andrés Bello, La metodología implementada para llevar este proyecto estuvo basado en el modelo de cascada, la cual permite la modularización de las tareas y el completo secuenciamiento de las actividades a llevar a cabo, en función de alcanzar los objetivos planteados. De igual manera, se realizaron preselecciones de herramientas IDS candidatas a cumplir con la tarea final de monitoreo sobre el entorno seleccionado para tales fines. Conjuntamente con la implantación del sistema IDS se estableció un modelo de políticas de seguridad orientadas a la correcta administración de la herramienta, para de esta forma garantizar un completo marco de seguridad sobre el entorno a proteger y los activos establecidos en su estructura.

En las conclusiones se estableció la implementación de Snort 2.0, como herramientas IDS la cual es una aplicación bajo filosofía de código abierto, brindando así a la Universidad la posibilidad de modificar el código en cualquier momento para ajustarlo a sus necesidades más específicas.

Lo anteriormente planteado, da como sustento a esta investigación lo que corresponde a la utilización de herramientas para implementar seguridad como lo son los IDS en especial Snort 2.0, por otro lado también contribuye en fijar bases para tomar en cuenta políticas para el resguardo de los activos.

Santos, L. (2001), realizó un trabajo en Bogotá-Colombia titulado “Guía para la evaluación de seguridad en un sistema”, el estudio presenta una serie de lineamientos básicos para la evaluación de seguridad en un sistema, con el objeto de articular diversos conceptos y técnicas para la identificación y valoración de riesgos. El objetivo fue exponer y presentar algunas reflexiones sobre tres métodos tradicionales para evaluar la seguridad de un sistema: análisis de riesgos, listas de chequeo y auditoria.

Entre las conclusiones se destaca que en Colombia las organizaciones y/o empresas no cuentan con registros acerca de los incidentes de seguridad, lo que dificulta la labor de determinar el impacto de los riesgos en términos económicos, necesitando considerarse en la mayoría de los casos una serie de

complicadas matrices para determinar el impacto de los riesgos en términos cualitativos de alto, medio o bajo, siendo esto, además, un proceso bastante polémico y desgastante en el interior de las organizaciones.

Como recomendación de seguridad fundamental a las empresas es importante empezar a llevar registros sobre incidentes de seguridad con el fin de dar mayor confiabilidad y mejorar los resultados en el ciclo de vida del análisis de riesgos.

Es indispensable retroalimentar el proceso de análisis de riesgos que obedecen a los siguientes: realización de cambios en el sistema, incidentes de seguridad y revisiones periódicas**.**

Son de vital importancia para el analista de seguridad informática la puesta en práctica de los métodos de checklist y auditoría para determinar controles ausentes en el sistema, ya que estas herramientas se basan en estándares mínimos de seguridad que debe cumplir todo sistema, la ausencia de alguno de ellos implica la recomendación inmediata del cumplimiento de ésta.

Es de destacar, la relación que guarda la presente investigación ya que presenta un análisis de las diversas metodologías para implantar seguridad en sistemas y valorar el impacto que causaría a un sistema la consecución de una amenaza.

Todos los trabajos citados anteriormente guardan relación entre sí y sirvieron de base para la investigación. Es de destacar, que todos señalan que la seguridad de la información es un factor de gran importancia para las empresas e instituciones ya que les proporciona integridad, confiabilidad y disponibilidad de los datos.

## Bases Teóricas

Dado que la presente investigación tuvo como objeto establecer un sistema de gestión de seguridad de la información para el Sistema Administrativo Integrado en la red de datos de la Universidad Nacional

Experimental Politécnica “Antonio José de Sucre”, Vicerrectorado de Puerto Ordaz, basado en el estándar ISO/IEC 27001:2005, se consideró relevante trabajarlo en base a algunos conceptos establecidos que intervienen en forma determinante en el tema como lo son: Seguridad Informática, Seguridad en los Sistemas Informáticos, Propiedades de la Seguridad Informática, Objetivos de la Seguridad, Términos de Riesgos, Factores de Riesgos, Análisis del Riesgo y su Evaluación, Medidas de Seguridad, Estandarización y Seguridad de las Tecnología de Información, Sistema de Gestión de Seguridad de la Información, ISO/IEC 27001:2005 y Herramientas para el Análisis de Riesgo.

### *Seguridad Informática*

La seguridad es definida por, Red (2002), como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, la información es el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

Existen otras definiciones importantes que se deben considerar al momento de hablar de seguridad informática, estas son:

*Activo:* recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos. Cualquier cosa que tenga valor para la organización (ISO/IEC 13335-1:2004)

*Amenaza:* es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

*Impacto:* consecuencia de la materialización de una amenaza.

*Riesgo:* posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

*Vulnerabilidad:* posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

*Ataque:* evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

*Desastre o Contingencia:* interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la normal operación de un negocio.

Es importante resaltar, aunque se puede entender que un riesgo y una vulnerabilidad se podrían englobar en un mismo concepto, una definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que la vulnerabilidad está ligada a una amenaza y el riesgo a un impacto. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Específicamente, Red (Ob. cit) señala que para los ataques de negación de servicio, el equipo de cómputo ya no es un blanco, es el medio a través del cual es posible afectar todo el entorno de red; es decir, anular los servicios de la red, saturar el ancho de banda o alterar el Web Site de la compañía. Con ello, es evidente que los riesgos están en la red y en menor grado en la computadora.

### *Seguridad en los Sistemas Informáticos*

La seguridad en los sistemas de información se ha convertido en algo imprescindible en toda empresa que gestione datos informáticos. La alta informatización de la sociedad actual ha conllevado el aumento de los denominados delitos informáticos. En este sentido, Garfinkel, S.y Spafford, G. citados por Hernández, E. (2003), señalan que un sistema informático es seguro

si se puede confiar en él y si se comporta de acuerdo a lo esperado. De allí, que la seguridad se basa por tanto en conceptos como la confianza y el acuerdo.

La seguridad es un conjunto de soluciones técnicas, métodos, planes, entre otros, con el objetivo de que la información que trata nuestro sistema informático sea protegida. Lo más importante es establecer un plan de seguridad en el cual se definan las necesidades y objetivos en cuestiones de seguridad. Es importante remarcar que la seguridad supone un costo y que la seguridad absoluta es imposible. Por lo tanto, hay que definir cuales son nuestros objetivos y a que nivel de seguridad se quiere llegar. Esto no es diferente a los planteamientos de seguridad en lo que se refiere a la protección física de una empresa o vivienda. Por ello, la seguridad se tiene que planificar haciendo un análisis del costo y su beneficio.

### *Propiedades de la Seguridad Informática*

Mendillo, V. (2001), señala los atributos o propiedades principales que debe brindar un sistema de seguridad:

*Confidencialidad (o secrecía)*: controlar quién puede leer la información (acceso) e impedir que información confidencial sea entregada a receptores no autorizados. Propiedad de que la información no esta disponible o divulgada a individuos, entidades o procesos no autorizados (ISO/IEC 13335-1:2004).

*Disponibilidad*: asegurar que los sistemas trabajan prontamente con un buen desempeño y garantizar protección y recuperación del sistema en caso de calamidades. Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada. (ISO/IEC 13335-1:2004)

*Integridad*: asegurar que la información recibida sea exactamente igual a la información enviada, es decir que no ha sido dañada por errores de transmisión o alterada intencionalmente en su contenido o en su secuencia. Propiedad de salvaguardar la exactitud y la totalidad de los activos. (ISO/IEC 13335-1:2004)

A*utenticidad*: garantizar que la información no es una réplica de información vieja la cual se quiere hacer pasar por información fresca, y que efectivamente proviene de una fuente genuina.

*Identificación y control de acceso*: Verificar la identidad de las personas. Autorizar y controlar quién y cómo se accede a los datos y los recursos de un sistema.

La confidencialidad y el control de acceso trabajan conjuntamente para proteger la información contra personas no autorizadas, mientras que permiten que los usuarios autorizados tengan acceso utilizando técnicas de identificación, usualmente por medio del nombre de usuario (*username*) más su contraseña (*password*). La integridad se garantiza por medio de bits de chequeo (*checksums*) que se añaden a la información y la autenticidad por medio de extractos (hash) y otros mecanismos.

Estas propiedades representan requerimientos que pueden ser enfatizados en diferentes proporciones para las diferentes aplicaciones. Para el sistema de defensa de una nación, la principal preocupación puede ser la confidencialidad de la información clasificada. Un sistema electrónico de transferencia de fondos puede requerir controles de integridad fuertes con menos énfasis en la confidencialidad. Ambas aplicaciones pueden tener la necesidad de autenticar que el receptor real de la información o del dinero depositado es el receptor a quien se le quiere enviar.

### ***Objetivos de la Seguridad***

La labor principal en seguridad informática es el aislamiento de los actos no deseables, y la prevención de aquellos que no se hayan considerado, de forma que si se producen hagan el menor daño posible. Al respecto, Amoroso, E. (2004), señala las distintas actividades que se deben llevar a cabo:

*Identificación de los usuarios:* Existen varias técnicas, entre las que se encuentran las contraseñas (passwords), o sistemas más sofisticados como reconocimientos del habla, huella dactilar o la retina del ojo.

*Detección de intrusos en la red.* Se debe detectar y actuar sobre cualquier acceso no autorizado a un sistema. El objetivo es la detección de intrusos en tiempo real, antes de que el sistema haya sido dañado seriamente.

*Análisis de riesgo*: Intenta cuantificar los beneficios obtenidos con la protección contra amenazas de seguridad. El riesgo es función de la frecuencia con la que se producen dichas amenazas, vulnerabilidad de la protección contra las mismas y las pérdidas potenciales que se produjesen en el caso de que se diese una.

*Clasificación apropiada de los datos.* En la gestión de seguridad llegan gran cantidad de datos provenientes de los últimos programas de control generados a partir de las actuaciones que llevan a cabo los usuarios en el sistema. Es importante para una buena supervisión de la seguridad, el clasificar los datos convenientemente, de tal forma que se ahorre tiempo en su análisis.

*Control de las nuevas aplicaciones.* Cuando se instala una nueva aplicación se debe comprobar que no introduzca nuevas brechas de seguridad especialmente si se ejecuta con permisos de root.

*Análisis de los accesos de los usuarios:* Es necesario tener un control para poder detectar intentos de acceso no autorizados.

### *Términos de Riesgo*

Como los riesgos existen en todas las actividades, la problemática en la seguridad de la información ha sido enfrentada con criterios tomados de otras disciplinas. Estos enfoques han dado lugar al uso de términos diferentes con significados no muy claros. Al respecto, Ormella (2007), señala los siguientes casos: a) Valorización del riesgo: analizar las amenazas a un sistema de información, las vulnerabilidades del mismo y el impacto potencial si se

concretan dichas amenazas. b) Evaluación del riesgo: valuación del riesgo respecto algún criterio de seguridad, por ejemplo una norma. c) Análisis de riesgo: Identificación y valuación de los niveles de riesgo de activos, amenazas y vulnerabilidades y d) Gestión de riesgo: Determinación de la estrategia efectiva en costo, del tratamiento y procedimientos a aplicar a partir de los resultados de la valuación, por ejemplo: 1) Aceptarlos, 2) Minimizarlos, identificando, seleccionando e implementando contramedidas (salvaguardas) para su reducción a niveles aceptables, y 3) Transferirlos.

### *Factores de Riesgo*

El riesgo es definido por Amoroso (2004) como la combinación de una amenaza que aprovecha alguna vulnerabilidad de un activo para impactarlo y causarle daño. En este mismo orden de ideas, Ormella (2007), señalas los siguientes factores de riesgos:

*Activos*: cualquier bien que necesite protección por lo que representa para una empresa, frente a posibles situaciones de pérdida de condiciones como son la Confidencialidad, Integridad o Disponibilidad (CIA). La ISO/IEC 13335-1:2004 define la confidencialidad como la propiedad de que la información no está disponible o divulgada a individuos, entidades o procesos no autorizados, la integridad es la propiedad de salvaguardar la exactitud y la totalidad de los activos y la disponibilidad es la propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada.

Es importante clarificar que es un activo de información. Según la ISO 17799:2005 un activo de información es algo a lo que una organización le asigna un valor y, por lo tanto, la organización debe proteger. Asimismo, los clasifica en las categorías siguientes: a) Activos de información (Datos, manuales de usuarios, entre otros), b) Documentos de papel (contratos), c) Activos de software (aplicación, software de sistemas, entre otros), d) Activos físicos (computadoras, medios magnéticos, entre otros), e) Personal (Clientes,

personal), f) Imagen de la compañía y reputación, g) servicios (comunicaciones, entre otros).

Como se observa, los activos de información son muy amplios. De allí que, Alberto (2007) señala que se debe estar conceptualmente claro de que es un activo de información y conocer las distintas posibles modalidades, para así poder realizar un correcto análisis y una evaluación del riesgo y, por ende, poder establecer adecuadamente el modelo ISO 27001:2005.

En la organización, el proceso de identificación y de tasación de activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en los procesos y subprocesos que abarca el alcance del modelo. Los activos se consideran y categorizar por su criticidad en cuanto a lo que significan para las operaciones. En general, el análisis tiende a establecer una cantidad de niveles que generalmente no baja de cinco y que en algunos casos puede llegar a diez.

*Vulnerabilidades:* Puntos débiles relacionados con los activos organizacionales, operacionales, físicos y de sistemas IT, en definitiva, todo lo que pueda facilitar la concreción de una amenaza. Los niveles se pueden estimar en función de: severidad, dado por los recursos necesarios para aprovechar la vulnerabilidad y el efecto en el activo, y el grado de exposición, extensión del efecto básico, facilitando la explotación de otras vulnerabilidades del mismo activo y/o se extiende a otros activos. Es usual trabajar con no más de tres niveles, especialmente cuando la determinación de una vulnerabilidad puede considerarse como subjetiva.

*Amenazas*: Acciones que pueden causar daño en un activo. Se las puede clasificar por ejemplo en las de fuerza mayor, deficiencias organizacionales, fallas humanas, fallas técnicas y actos deliberados. Los niveles pueden estimarse de acuerdo a la capacidad y motivación del agente provocador (salvo en el caso de la fuerza mayor). En general puede ser tres o cinco. La concreción de una amenaza provoca un impacto en un activo. Dicho impacto y la

probabilidad de ocurrencia a lo largo de cierto tiempo pueden usarse como medida del efecto de una amenaza.

### *Análisis del riesgo y su Evaluación*

El análisis del riesgo es la utilización sistemática de la información para identificar las fuentes y estimar el riesgo (ISO/IEC Guide 73:2002). En este mismo orden de ideas, Gallo, I y otros (2003), señalan que la primera pregunta a la hora de diseñar y planificar la seguridad en un sistema informático es la de analizar los riesgos. El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

La organización debe decidir el método para hacer el cálculo del riesgo que sea apropiado para la empresa y los requerimientos de seguridad. Los niveles de riesgo calculados proveen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.

Ormella, (ob. cit) señala que el análisis de riesgo se realiza con diferentes metodologías que en general se encuadran en una de dos formas: análisis cuantitativo o cualitativo. El cuantitativo trabaja con valores monetarios, lo cual facilita la comprensión y la variante cualitativa trabaja con niveles no numéricos, es más simple pero menos precisa.

Una vez efectuado el cálculo del riesgo por cada activo, en relación de su amenaza, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más significativos. Este proceso se denomina evaluación del riesgo (Alberto, 2007). Luego, de analizar los riesgo, se debe iniciar un proceso de

toma de decisiones con respecto a cómo se tratará el riesgo. Es de destacar, que la decisión esta influenciada por dos factores: a) El posible impacto si el riesgo se pone de manifiesto y b) que tan frecuente puede suceder. Estos factores dan una idea de la pérdida esperada si el riesgo ocurriera, si nada se hiciera para mitigar este riesgo. El autor, señala las siguientes estrategias para el tratamiento del riesgo:

*Reducción del riesgo*: Para todos aquellos riesgos donde la opción de reducirlos se ha tomado, se deben implementar controles apropiados para poder reducirlos al nivel que se haya definido como aceptable. Estos controles pueden reducir el riesgo estimado en dos maneras: reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza y reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados, reaccionando y recuperándose de ellos.

*Aceptar el riesgo*: Muchas veces se presenta la situación en la cual la organización no encuentra controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias la decisión de aceptar los riesgos y vivir con las consecuencias es la más adecuada.

*Transferencia del riesgo*: la transferencia del riesgo es una opción cuando es difícil reducir o controlar el riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante estas circunstancias. En este sentido, existe una serie de mecanismos para transferir los riesgos a otra organización; por ejemplo, utilizar una aseguradora o la utilización de terceros para manejar activos o procesos críticos, en la medida en que tengan capacidad de hacerlo. Es importante señalar, que el riesgo residual siempre estará presente y la responsabilidad por la seguridad de la información y por las instalaciones para el procesamiento de información, al hacerse mercerizado éstas, siempre le corresponde a la organización original.

*Evitar el riesgo*: por el modo de evitar el riesgo se entiende cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una

actividad comercial en particular, para así evitar la presencia del riesgo. El riesgo puede evitarse por medio de: no desarrollar ciertas actividades comerciales (por ejemplo: la no utilización de Internet), mover los activos de un área de riesgo y decidir no procesar información particularmente sensitiva.

### *Medidas de Seguridad*

Uno de los factores claves en el mantenimiento de la seguridad es la selección de las medidas de seguridad. La selección de medidas depende de varios factores, como el entorno, las expectativas, el valor de los activos, el presupuesto, entre otros.

Aceituno (2004), señala que al decidir cuáles son las mejores medidas de seguridad para una organización, se debe tener en cuenta: a) Existe un riesgo residual que no puede eliminarse, b) Toda medida será un compromiso entre nivel de protección, eficacia, facilidad de gestión, coste, entre otros. No hay medidas perfectas. c) Es mejor una solución buena hoy que una "perfecta" mañana. d) Para poder confiar en una medida debemos ponerla periódicamente a prueba y e) El coste de la selección de una medida de seguridad debería ser despreciable en comparación con el coste de la medida.

Las medidas de seguridad son controles de seguridad, dispositivos o acciones que actúan de manera: 1) Preventiva: previenen incidentes y por consiguiente disminuyen la vulnerabilidad a amenazas conocidas. Se pueden mencionar las normas, procedimiento, auditorias, firewall, IDS (Sistemas de detección de intrusos), Corta fuegos externos, candados, control de accesos, escaneado de virus y contenido, encriptación, entre otros; 2) Correctivos: Medidas que disminuyen el impacto, y por tanto protegen tanto contra amenazas previsibles como imprevisibles: Sistemas redundantes, RAID, copia de respaldo, centro de respaldo, líneas de comunicación redundantes, cluster. DMZ y 3) Doble efecto: Actúan de ambas formas, concientización,

capacitación, Planes de Continuidad de Negocios (BCP), Planificación de Recuperación de desastres (DRP) y Planes de Contingencia.

### *Estandarización y seguridad de la tecnología de la información*

García P. (2005), señala que en lo referente al marco internacional que se ocupa de los aspectos relacionados con las tecnologías de la información, existe un comité conjunto constituido entre los dos organismos internacionales de normalización, ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional, que se centra en los aspectos eléctricos de cada campo). Este comité conjunto Nº 1 es el denominado JTC1 (Joint Technical Committee 1), en este órgano participan 68 países, entre ellos España, a través de AENOR (Asociación Española de Normalización y Certificación) que asumió su responsabilidad internacional en ISO en 1987 y en IEC en 1995, representando los intereses españoles en el campo de la normalización internacional ante dichas organizaciones.

En el ámbito del Comité ISO/IEC/JTC 1 se considera la especificación, diseño y desarrollo de sistemas y herramientas que tratan la información en sus distintos aspectos: captura, representación, proceso, seguridad, transmisión, intercambio, presentación, direccionamiento, organización, almacenamiento y recuperación.

Este órgano de trabajo está estructurado en una serie de subcomités dedicado cada uno de ellos a un aspecto específico de las TI; en concreto el que ocupa el número 27 es el responsable de todos los aspectos de seguridad, denominándose JTC1/SC27 "Técnicas de Seguridad". En la actualidad cuenta con más de 40 países miembros. En el JTC1 existe también un órgano denominado Information Technology Task Force (ITTF) responsable de la planificación cotidiana y coordinación del trabajo técnico del mismo, y de la aplicación de los Estatutos y los Procedimientos de ISO e IEC.

Por otra parte, La Universidad Nacional de Colombia y esCERT Universidad Politécnica Catalunya (2005) señalan que existen varios estándares internacionales relacionados con seguridad informática que se consideran importantes en la actualidad.

Para la administración de seguridad de la información: La Internet Engineering Task Force (IETF) elaboró el RFC2196 Site Security Handbook, que ofrece una guía práctica para quienes intentan asegurar servicios e información.

El estándar británico BS 7799 es un estándar aceptado ampliamente que ha sido utilizado como base para elaborar otros estándares de seguridad de la información, incluyendo el ISO 17799 y el ISO 27001.

Entre los estándares para evaluación de seguridad en sistemas, se tiene: IS 15408 elaborado por la Organización Internacional para la Estandarización (ISO, International Standardization Organization). Este estándar, The Common Criteria for Information Technology Security Evaluation v2.1 (ISO IS 15408) es una mezcla mejorada de ITSEC, el Canadian criteria, y el US Federal Criteria.

En toda organización que haga uso de las tecnologías de información es recomendable implementar prácticas de seguridad, disminuyendo así el riesgo de pérdida de información. En este sentido, Red (2002), señala que el estándar internacional de alto nivel para la administración de la seguridad de la información es el ISO 17799, este estándar, fue publicado por la ISO (International Organization for Standardization) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones.

El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática: a) C*onfidencialidad.* Asegurar que únicamente personal autorizado tenga acceso a la información. b) *Integridad.* Garantizar que la información no será alterada,

eliminada o destruida por entidades no autorizadas y c) *Disponibilidad*. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación; el objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

El éxito de la implementación del estándar de seguridad ISO 17799 requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta.

Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad, cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

La correcta selección de los controles es una tarea que requiere del apoyo de especialistas en seguridad informática, con experiencia en la implementación del ISO 17799, ya que cuando éstos se establecen de forma inadecuada pueden generar un marco de trabajo demasiado estricto y poco adecuado para las operaciones de la organización.

Córdova, G. (2004), señala que la norma ISO 17799 corresponde a una norma internacional que establece; que la información es un activo y requiere de una protección adecuada. Este estándar ofrece recomendaciones para realizar una debida gestión en la seguridad de la información, (definición, implementación, manutención).

Proteger adecuadamente la información es poder asegurar la continuidad del negocio, proporciona una base común para desarrollar normas de seguridad

que corresponden a un conjunto de controles, a ser evaluados al implementar sistemas de gestión de seguridad.

Uno de los aspectos importantes de esta norma es que propone metodologías, pero no tiene la facultad de ser certificable.

Igualmente, el autor señala que la norma BS7799-2:2002, es la Parte II de lo que fue el primer sistema de seguridad propuesto en el 95 (BS7799) y complementa a la Parte I, que corresponde a la ISO17799. Esta metodología de normalización se basa en el modelo Plan-Do-Check-Act., metodología base del ISMS y es reconocido a nivel internacional.

Esta norma (BS7799-2:2002) es reconocida por organismos internacionales acreditados y su proceso dura aproximadamente entre 2-4 años, ambas normas son un conjunto de controles considerados una buena práctica en la seguridad de la información, y que incluyen: políticas, procedimientos, estructura Organizacional y funciones de Software.

## Sistema de Gestión de Seguridad de Información

Alberto (2007), señala que hoy en día, dada la competencia que la globalización y las nuevas reglas del comercio internacional han generado, las empresas, no importa su tamaño, la industria en la que estén ubicadas o su naturaleza, tienen que ser creativas e innovadoras para poder mantenerse en los mercados y poder aumentar su competitividad. Pero una empresa creativa e innovadora no puede asegurar que sus nuevos diseños prototipo lleguen primero antes que la competencia al mercado.

Muchas veces sucede que otra empresa se adelante y sale primero con el producto al mercado, pero, en muchas ocasiones, en la empresa hay fuga de información y los secretos llegan rápidamente a manos inescrupulosas que venden esa información al mejor postor.

En las empresas, el escenario descrito es algo que se presenta de manera cotidiana. Muchas veces la información deja de ser confidencial y muchas

personas sin autorización tienen acceso a ella. La ingeniería social en las empresas no tiene fronteras para obtener la información que, por lo general, es de “alta confidencialidad”.

El problema es muy serio. En el siglo XXI, cuando la gestión del conocimiento es una característica vital en las empresas, se debiera tener formas de poder minimizar el riesgo de que la información se fugue, se altere o simplemente no esté disponible cuando se requiera. Al respecto, es conveniente conocer las respuestas a las siguientes interrogantes ¿Qué hacen las empresas para asegurar continuidad ante el impacto de un desastre?, por ejemplo, ¿qué le pasaría a una empresa financiera, si su servidor quedara fuera de servicio? ¿Qué pasaría si la base de datos de la empresa se pierde? Todos estos escenarios de amenazas pueden ponerse de manifiesto y hacer colapsar a cualquier empresa, si no se tiene una estrategia de continuidad claramente definida por cada escenario de amenazas previamente identificado, y un plan de reanudación de operaciones que permita operacionalizar rápidamente la estrategia de continuidad del negocio, sin que la empresa colapse financiera y operacionalmente.

Para proteger la información en las empresas se debe identificar los activos de información que tienen impacto en el negocio, hacerles un análisis y evaluación del riesgo y decidir cuáles son las opciones de tratamiento del riesgo a implantar para minimizar las posibilidades de que las amenazas puedan causar daño y no penetren a la organización.

Lo anteriormente planteado, son las acciones que un “Sistema de Gestión de Seguridad de Información” (SGSI) busca instaurar en una empresa. Un SGSI puede definirse de varias maneras:

Albert y Dorofree, (2003), lo define como un establecimiento de un sistema que determine que requiere ser protegido, y por qué, de qué debe ser protegido y cómo protegerlo.

Asimismo, Peltier (2001), la define como la preservación de la confidencialidad, integridad y disponibilidad de la información.

El modelo ISO 27001:2005 define a un SGSI como “la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información”. Además de esto, el ISO 27001:2005 define la seguridad de la información como la “preservación de la confidencialidad, integridad, no repudio y confiabilidad”. A continuación se hace referencia a la Norma ISO 27001:2005, la nueva familia 27000.

**ISO/IEC 27001:2005**

El origen es británico y en el año 2005, la Organización Internacional para la Normalización (ISO) la oficializó como norma. La figura 1, la historia del ISO 27001 a lo largo del tiempo.

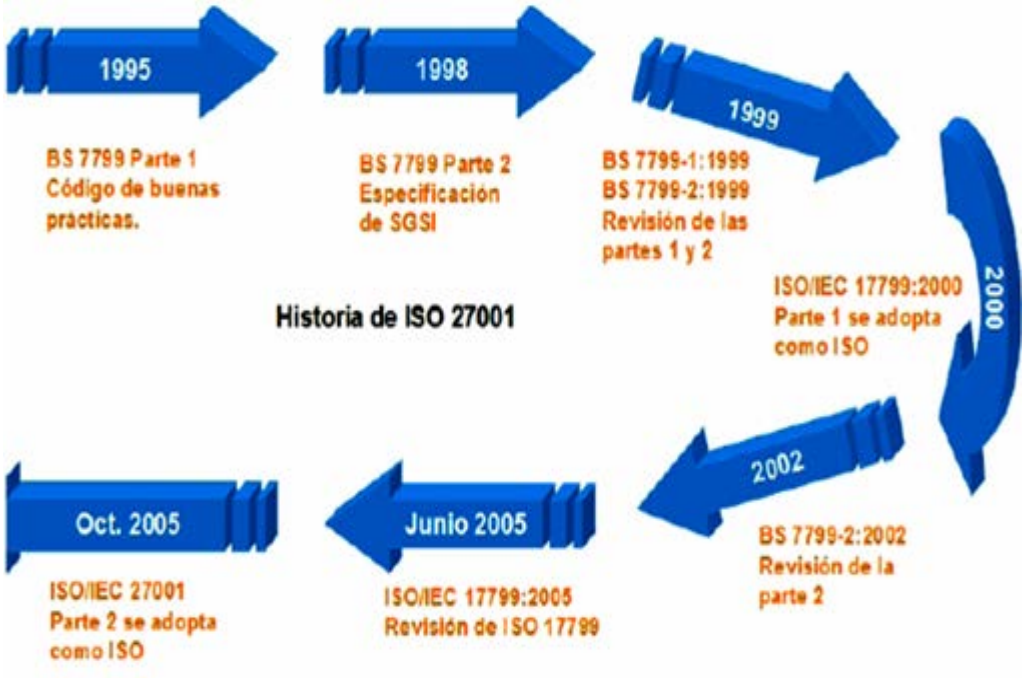



**Figura 1:**Historia de ISO 27001. **Fuente:** http://www.iso27000.es

En Marzo de 2006, posteriormente a la publicación de la ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información. Esta servirá como base a la ISO 27005.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares, estructurada como se muestra en la siguiente figura 3:

| | | |
|---|---|---|
| **ISO 27000 SGSI "Fundamentos y vocabularios"** | **ISO/IEC 27001:2006 Requerimientos** | **ISO/IEC 27002:2007 (ISO 17799: 2005)** |
| **ISO/IEC 27003 "Lineamientos para la Implementación"** | **ISO/IEC 27004 Lineamientos "Métrica y Mediciones"** | **ISO/IEC 27005 SGSI Lineamientos "Gestión del riesgo"** |

**Figura 2:** Familia de estándares de la ISO 27000: **Fuente:** Autora: 2007

La ISO 27000: En fase de desarrollo. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma será gratuita, a diferencia de las demás de la serie, que tendrán un costo asociado.

La ISO 27001: Es la norma principal de requisitos del sistema de gestión de seguridad de información. Tiene su origen en la BS 7799-2:2002 y es la norma con la cual los SGSI de las organizaciones son certificados por auditores externos. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A (ver anexo F), enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 17799:2005 (futura ISO 27002), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de

todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

La ISO 27002 (ISO 17799:2005): En desarrollo, probable publicación a finales de 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a la seguridad de información. No es certificable. Será la sustituta de ISO 17799:2005, que es la que está actualmente en vigor, y que contiene 39 objetivos de control y 133 controles agrupados en 11 dominios.

ISO 27003: En fase de desarrollo; probable publicación a finales de 2008. Contendrá una guía de implementación de un SGSI e información acerca de uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004: En fase de desarrollo; probable publicación a lo largo de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (implementar y utilizar) del ciclo PDCA.

ISO 27005: En fase de desarrollo; probable publicación a finales de 2007 ó principios de 2008. Consistirá en una guía para la gestión del riesgo de la seguridad de información y servirá, por lo tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Se basará en la BS 7799-3:2006.

ISO 27006: Publicada en Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoria y certificación de los SGSI.

Esta norma adopta un enfoque basado en procesos para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar el SGSI de una organización.

Una organización necesita identificar y gestionar muchas actividades a fin de funcionar eficazmente. Cualquier actividad que utiliza recursos, y que se

gestiona con el fin de permitir que los elementos de entrada se transformen en resultados, se puede considerar como un proceso. Frecuentemente el resultado de un proceso constituye directamente el elemento de entrada del siguiente proceso

El enfoque basado en procesos para la gestión de seguridad de la información enfatiza la importancia de: a) La comprensión de los requisitos de seguridad de la información de una organización y la necesidad de establecer la política y objetivos para la seguridad de la información. c) Realizar seguimiento y revisar el desempeño y eficacia del SGSI y d) La mejora continua con base en mediciones objetivas.

Esta norma adopta el modelo "Planificar – Hacer – Verificar – Actuar" (PHVA, el cual es aplicado para estructurar todos los procesos del SGSI. La Figura 3 ilustra cómo un SGSI toma como entrada los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios para producir resultados de seguridad de la información que cumplan esos requisitos y expectativas.

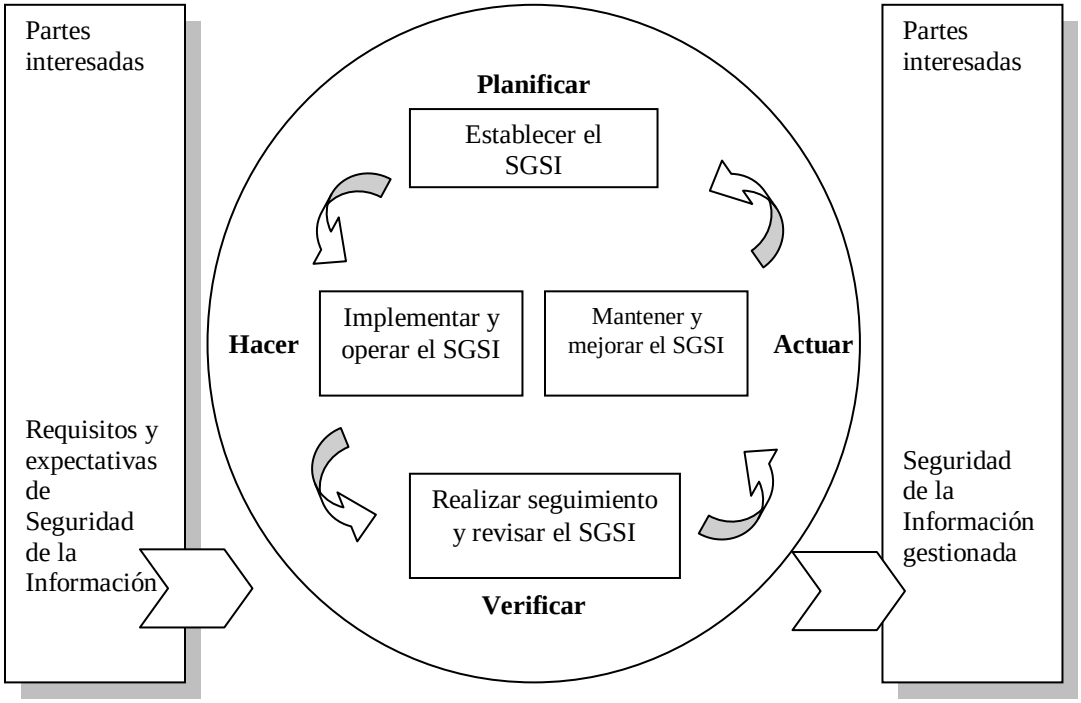



**Figura 3.** Modelo de PHVA aplicado a los procesos del SGSI. ISO/IEC 27001:2005

La adopción del modelo de PHVA también reflejará los principios según lo precisado en las directrices OECD (2002) que gobiernan la seguridad de los sistemas y redes de información. Esta norma provee un modelo robusto para implementar los principios en aquellas directrices que gobiernan la evaluación del riesgo, el diseño e implementación de la seguridad, la gestión y reevaluación de la seguridad.

El modelo PHVA se explica de la siguiente forma: a) Planificar: Establecer la política, objetivos, procesos y procedimientos pertinentes del SGSI para gestionar el riesgo y mejorar la seguridad de la información para entregar los resultados de acuerdo con las políticas y los objetivos globales de una organización. b) Hacer: Implementar y operar la política, controles, procesos y procedimientos del SGSI. c) Verificar: Evaluar y, donde sea aplicable, medir el desempeño del proceso frente a la política, objetivos y experiencia práctica del SGSI e informar sobre los resultados a la dirección para la revisión y d) Actuar: Tomar las acciones correctivas y preventivas, sobre la base de los resultados de la auditoria interna del SGSI y la revisión por la dirección u otra información pertinente, para lograr la mejora continua del SGSI.

El ISO/IEC 27001:2005 está diseñado para que sea compatible con el ISO 9001:2000 y con el ISO 14001:2004.

En este sentido, Alberto, A. (2007), señala que el modelo ISO 27001:2005 está diseñado bajo una óptica de enfoque a procesos. El SGSI está conceptualizado para funcionar en cualquier tipo de organización, operando bajo el enfoque de procesos. En la figura 4, se ilustra la presentación de los distintos componentes del modelo ISO 27001:2005, bajo la perspectiva de procesos.

El modelo está concebido para que opere con base en insumos provenientes de clientes, proveedores, usuarios, accionistas, socios y otras partes interesadas.

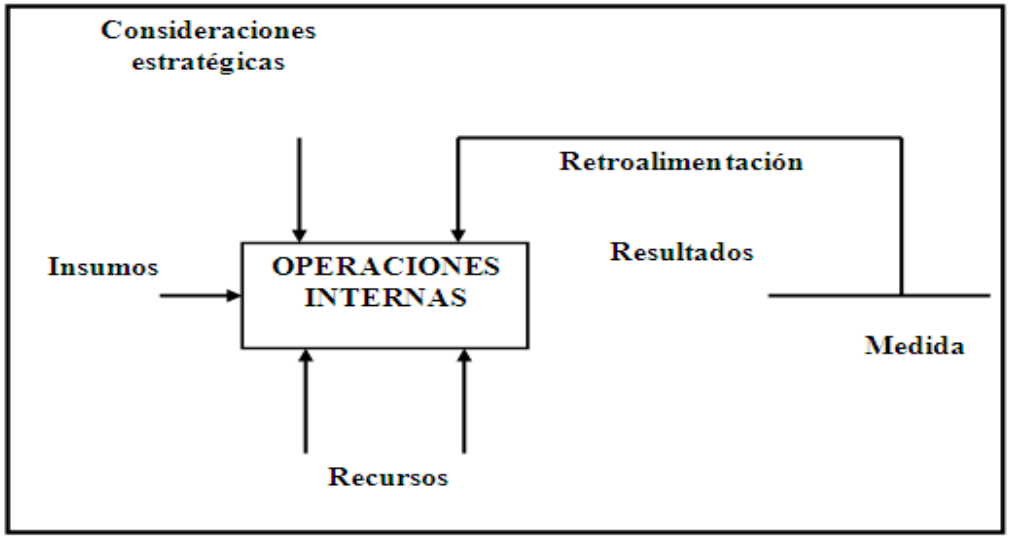



**Figura 4.** Enfoque a procesos del ISO 27001:2005 **Fuente:** Alberto, A. (2007)

Estos insumos, a través de las operaciones internas del SGSI proporcionan resultados concretos del desempeño del SGSI. La norma exige que el mecanismo de retroalimentación para controlar el desempeño del SGSI se establezca y se diseñe métrica para, por medio de indicadores, poder medir su desempeño.

El enfoque a procesos del SGSI también contempla los recursos que deben ser provistos para que las operaciones internas funcionen adecuadamente.

El modelo ISO 27001:2005, en su óptica de procesos, también permite que cada organización influencie el desempeño del modelo a través de consideraciones estratégicas, tales como objetivos y políticas particulares de la firma.

## Herramientas para el análisis de riesgo

En el mercado existen varias herramientas para realizar el análisis de riesgos, entre las de carácter propietario se destacan:

CRAMM, producto de Insight Consulting, que puede usarse con ISO 27001 así como para el manejo de riesgo de negocios. Para el análisis de riesgo se recolectan datos en reuniones y entrevistas con cuestionarios estructurados. Tiene tres partes: 1) Valorización de activos, en escala de 1 a 10. 2) Evaluación de amenazas y vulnerabilidades. Niveles de 1 a 5 para las amenazas, y de 1 a 3 para las vulnerabilidades y 3) Cálculo del riesgo, de 1 a 7 según una matriz. Más de 3000 contramedidas estructuradas en base de datos y que pueden priorizarse.

COBRA (Análisis de Riesgo Objetivo y Bifuncional), desarrollada por C & A Systems en cooperación con instituciones financieras. Especialmente prevista para verificar el cumplimiento de las normas ISO 17799/27001. Provee un completo análisis de riesgo, compatible con la mayoría de las metodologías conocidas cualitativas y cuantitativas. Lo forman varios programas: Risk Consultant, el principal, incluyen las bases de conocimiento que se personalizan y modifican con el Module Manager.

RA2 Art of Risk: Producto de Aexis y Xisec trabaja con análisis cualitativo de riesgo basado en modelado estadístico. Desarrollado conforme la ISO 17799 y la ISO 27001, usa también los principios contenidos en la MICTS-2. Permite seleccionar los controles ISO 17799 y producir evidencia a los auditores que se han llevado a cabo los pasos de la ISO 27001 para certificación. Produce directamente el SoA adecuado para la certificación ISO 27001.

MAGERIT: del Ministerio de las Administraciones Públicas (MAP) de España. La aplicación se puede ver en cuatro etapas: planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas. En la versión 2.0, la documentación consta de tres partes: 1) Método. Análisis y gestión de riesgos, proyectos. 2) Catálogo de Elementos. Amenazas y salvaguardas y 3) Guía de Técnicas. Tipo de análisis, diagramas, planificación de proyectos.

Igualmente existen herramientas de libre acceso, entre las que se destacan:

OCTAVE. Evaluación de factores operacionalmente críticos: amenazas, activos de sistemas y personal, y vulnerabilidades. Hay dos versiones: Octave y Octave-S (Small, pequeñas empresas); éste último para equipos pequeños de personal de seguridad. El Octave-S define una técnica de valuación basada en riesgos, desarrollada en 10 volúmenes. El proceso incluye tres fases: construcción de perfiles de amenazas en base a los activos, identificación de la infraestructura de las vulnerabilidades, y desarrollo de la estrategia y planes de seguridad.

Threat and Risk Assesment Working Guide (Canadá). Considera vulnerabilidades de sistemas, personal, objetos y externas, con cinco niveles como resultado de tres niveles de severidad y tres de exposición. Trabaja con cinco niveles de amenazas, caracterizando los agentes de amenazas en tres niveles de capacidad y otros tres de motivación- incorpora los escenarios de amenazas, donde estipula analizar el impacto en función de la sensibilidad de los activos y tasa de vulnerabilidad, así como de la frecuencia de ocurrencia. No define bien los riesgos finales.

Guideline del NSW de Australia. Tiene tres partes: Una revisión del proceso de gestión de riesgo, ejemplo de amenazas y vulnerabilidades y una guía para la selección de los controles de seguridad. Incluye una tabla que relaciona cada control de la norma ISO 17799:2000 con diferentes tipos de control: protección, prevención, detección, respuesta y recuperación. Y otra tabla relaciona cada control con los parámetros CIA: Confidencialidad, Integridad y Disponibilidad, así como también con la Autenticación, Responsabilidad y Confiabilidad.

El IT Baseline Protección Model del BSI Alemán, permite establecer los riesgos en base a los activos, amenazas y contramedidas. No trabaja directamente con vulnerabilidades. Clasifica los activos en 35 tipos en 7 categorías, las amenazas un total de 200 con cinco tipos: Fuerza mayor, Deficiencias organizacionales, Fallas humanas, Fallas técnicas y Actos

deliberados. Contramedidas: Unas 600 de diferentes tipos. Incluye tabla de contramedidas vs. amenazas.

En relación a lo antes expuesto y para efectos de esta investigación se trabajó con las herramientas CRAMM y BSI Alemán.

## Bases Legales

Los planteamientos legales se basaron en los lineamientos, normas, procedimientos y estándares que establecen los artículos que tienen correspondencia con esta investigación y que se encuentran en:

### *Estándares Internacionales*

ISO/IEC 27001:2005 – Tecnología de la Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la _Información.

ISO/IEC 17799:2005 – Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información Organización Internacional de Estándares (ISO).

Directrices OECD (2002), para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad.

### *Leyes Nacionales*

La Constitución Bolivariana de la República de Venezuela (1999), en su artículo 110, señala que el Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional.

Ley Especial Contra Delitos Informáticos promulgada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001 por la Asamblea Nacional, Caracas –

Venezuela, la cual refiere en el artículo 1, que el objeto es la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley. Además, señala las sanciones por los delitos cometidos contra los Sistemas de Información en los artículos 6, 7, 8, 9, 11, 12, 13 y 14.

Ley Orgánica de Telecomunicaciones, promulgada en Gaceta Oficial Nº 37.148 de fecha 28 de febrero de 2001 por Decreto Nº 1.024 - 10 de febrero de 2001, Caracas – Venezuela, esta tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a fin de garantizar el derecho humano de las personas a la comunicación y a la realización de las actividades económicas de telecomunicaciones necesarias para lograrlo, sin mas limitaciones que las derivadas de la Constitución y las leyes.

### *Normativa Interna*

Resolución de Consejo Universitario No. 2004-E14-06. Lineamientos de Tecnología y Servicios de Información de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" aprobado el 20 de julio del 2004. Barquisimeto – Venezuela.

Resolución de Consejo Universitario No. 2005-E09-05 Reglamento de Tecnología y Servicios de Información de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" aprobado el 04 de Mayo del 2005. Barquisimeto – Venezuela, este reglamento establece las directrices y normas que rigen las actividades relacionadas con la Tecnología y Servicios de Información que se requieren realizar en la universidad como apoyo a la gestión Académica, Administrativa y de Extensión, artículos 6, 7, 8, 35 y 39.

## Sistema de Variable

Según Hernández, R. y otros (2003), una variable "es una propiedad que puede variar y cuya variación es susceptible de medirse u observarse" (p. 143). En este sentido las variables deben ser definidas en dos formas conceptual y operacionalmente.

Una definición conceptual trata la variable con otros términos, para ello se deben definir las variables que se usan en forma tal que puedan ser comprobadas o contextualizadas. Lo anterior es posible usando lo que se conoce como definiciones operacionales. Una definición operacional constituye el conjunto de procedimientos que describe las actividades que un observador debe realizar para recibir las impresiones sensoriales, las cuales indican la existencia de un concepto teórico en mayor o menor grado.

En el presente trabajo la variable a definir es Sistema de Gestión de Seguridad de la Información y a continuación se describe operacionalmente basado en los objetivos de control de las normas ISO/IEC 27001:2005.

**Cuadro 1**

**Operacionalización de las Variables**

| Variable | Dimensión | Indicadores | Ítems | Instrumento |
|---|---|---|---|---|
| Sistema de Gestión de seguridad de la Información | Políticas de Seguridad | Documento de la política de seguridad de la información | 1 | CUESTIONARIO Y OBSERVACIÓN DIRECTA |
| | | Revisión de la política de Seguridad de la Información | 2 y 3 | |
| | Organización de la Seguridad de la Información | Compromiso de la dirección para la seguridad de la información | 4 y 5 | |
| | | Asignación de responsabilidades sobre seguridad de la información | 6 | |
| | | Proceso de autorización para los recursos de procesamiento de la información | 7 | |
| | | Acuerdos de confidencialidad | 8 | |
| | | Identificación de riesgos relacionados a partes externas. | 9 y 10 | |

**Cuadro 1. Continuación**

| Variable | Dimensión | Indicadores | Ítems | Instrumento |
|---|---|---|---|---|
| Sistema de Gestión de seguridad de la Información | Gestión de activos | Inventario de equipos | 11 y 12 | CUESTIONARIO Y OBSERVACIÓN DIRECTA |
| | | Propiedad de los activos | 13 | |
| | | Directrices de clasificación | 14 | |
| | | Selección | 15 | |
| | Seguridad de recursos humanos | Proceso disciplinario | 16 | |
| | | Toma de conciencia, educación y formación en la seguridad de la información | 17 | |
| | | Devolución de los activos | 18 y 19 | |
| | Seguridad física y ambiental | Perímetro de seguridad | 20 | |
| | | Controles físicos de entrada | 21 - 25 | |
| | | Protección contra las amenazas externas y ambientales | 26 y 27 | |
| | | Trabajo en áreas seguras | 28 | |
| | | Ubicación y protección del equipo | 29 | |
| | | Servicio de apoyo | 30 | |
| | | Seguridad del cableado | 31 | |
| | | Mantenimiento de equipos | 32 | |
| | | Seguridad en la reutilización o eliminación de equipos | 33 | |
| | | Retiro de la propiedad | 34 | |
| | Gestión de comunicaciones y operaciones | Documentación de procedimientos operativos | 35 | |
| | | Gestión de cambio | 36 | |
| | | Gestión de la capacidad | 37 | |
| | | Controles contra código malicioso | 38 y 39 | |
| | | Copia de seguridad de la información | 40 - 42 | |
| | | Control de red | 43 | |
| | | Disposición de medios | 44 y 45 | |
| | Gestión de comunicaciones y operaciones | Registro de auditoria | 46 | |
| | | Registro de fallas | 47 | |
| | | Sincronización de relojes | 48 | |
| | Control de accesos | Política de control de acceso | 49 | |
| | | Registro de usuarios | 50 | |
| | | Gestión de contraseñas de usuario | 51 | |
| | | Uso de contraseñas | 52 | |
| | | Sesión inactiva | 53 | |
| | | Restricción de acceso a la información | 54 | |

**Cuadro 1. Continuación**

| Variable | Dimensión | Indicadores | Ítems | Instrumento |
|---|---|---|---|---|
| Sistema de Gestión de seguridad de la Información | Adquisición, desarrollo y mantenimiento de sistemas de información | Análisis y especificación de los requisitos de seguridad | 55 | CUESTIONARIO Y OBSERVACIÓN DIRECTA |
| | | Validación de datos de entrada | 56 | |
| | | Control de procesamiento interno | 57 | |
| | | Validación de los datos de salida | 58 | |
| | | Política sobre la utilización de controles criptográficos | 59 | |
| | Gestión de incidente de seguridad de la información | Reporte de los eventos de seguridad de información | 60 | |
| | | Reporte de debilidades de seguridad | 61 | |
| | | Responsabilidades y procedimientos | 62 | |
| | | Aprendizaje de los incidentes de seguridad de la información | 63 | |
| | Gestión de continuidad del negocio | Continuidad del negocio y evaluación de riesgo | 64 | |
| | | Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información | 65 | |
| | Cumplimiento | Identificación de la legislación aplicable | 66 | |
| | | Derechos de propiedad intelectual (DPI) | 67 | |
| | | Protección de los registros de la organización | 68 | |
| | | Controles de las herramientas de auditoria de los sistemas de información | 69 | |

Autora (2007)

# CAPITULO III

# MARCO METODOLOGICO

## Naturaleza del Estudio

El presente trabajo se ubicó en la modalidad de estudios de proyecto apoyado tanto en una investigación de campo como en la investigación monográfica documental, ya que según el Manual para la Elaboración del Trabajo Conducente al Grado Académico de: Especialización, Maestría y Doctorado (2002), se pretende dar una alternativa de solución a un problema de tipo institucional como es el establecimiento de un Sistema de Gestión de Seguridad de la Información para un sistema de información tomando como caso de estudio el Sistema Administrativo Integrado SAI en producción en la red de datos de la Unexpo Vicerrectorado de Puerto Ordaz y como norma la ISO/IEC 27001:2005. A continuación se describe la metodología utilizada.

## Diseño de Investigación

A fin de operacionalizar el presente estudio por medio de esta modalidad, se describen a continuación las tres primeras fases. La Fase I Diagnóstico, la Fase II de Factibilidad y la Fase III Diseño del Proyecto que se refiere a cada uno de los aspectos que contiene la propuesta. Es de resaltar, que la Fase IV de Ejecución y Evaluación corresponden a las autoridades de la Unexpo Vicerrectorado de Puerto Ordaz.

### *Fase I. Diagnóstico*

A través de esta fase se realizó el análisis general de la situación actual de la seguridad de la información; para ello se desarrollaron las primeras etapas de la metodología de análisis de información, a través de la aplicación de una investigación de campo al personal administrativo que opera el Sistema Administrativo Integrado SAI, pertenecientes a los departamentos de: Unidad de Finanzas y tesorería, Presupuesto, Almacén, Unidad de Compra, y Contabilidad y al personal técnico de la Coordinación de Producción y Operaciones de la ORTSI, de la Unexpo Vicerrectorado Puerto Ordaz, los cuales son los beneficiarios directos y hasta indirectos con la ejecución del proyecto.

#### *Población y Muestra*

Según, Balestrini (1998), una población o universo "puede estar referido a cualquier conjunto de elementos de los cuales pretenden indagar y conocer sus características, o una de ellas, y para el cual serán válidas las conclusiones obtenidas en la investigación" (p.56).

En este sentido, la autora plantea que para seleccionar la población, es necesario considerar cuál será la unidad de análisis, lo que permitirá definir con qué elementos (personas) se va a trabajar. En el caso de la presente investigación la población que determinó la necesidad de establecer un sistema de gestión de seguridad de la información para un sistema de información en producción en una red de datos, estuvo constituido por veintiséis (26) empleados administrativos que laboran en los diferentes departamentos donde están los módulos del Sistema Administrativo Integrado SAI, señalados a continuación en el cuadro 2.

En cuanto a la muestra, definida por Hernández et al. (2003) como un subconjunto de elementos que pertenecen al conjunto definido como población.

Igualmente, se tomó en cuenta lo expresado por Ary (1996), quien señala que "...si la población posee pequeñas dimensiones, deben ser seleccionados en su totalidad, para así reducir el error en la muestra" (p.54); tomando como fundamento ésta definición, se puede inferir que la muestra es aquella representada por la totalidad de los individuos que permiten obtener información sobre el tema a investigar.

**Cuadro 2**

**Descripción de la Población**

| Departamento u Oficina | Cantidad |
|---|---|
| ORTSI | 3 |
| Unidad de Finanzas y Tesorería | 5 |
| Contabilidad | 5 |
| Presupuesto | 6 |
| Compra | 5 |
| Almacén | 2 |
| **Total** | **26** |

Autora (2007)

De lo anterior se deduce que los sujetos de estudio de la presente investigación estuvo conformado por veintiséis (26) personas que laboran en las unidades y departamento administrativos que operan con el Sistema Administrativo Integrado SAI, así como también el personal técnico del grupo de Soporte Servicios de Información (SSI), de la Coordinación de Producción y Operaciones (CPO) de la Oficina Regional de Tecnología y Servicios de Información (ORTSI) de la Unexpo, Vicerrectorado de Puerto Ordaz.

*Técnicas e Instrumentos de Recolección de Datos*

La técnica utilizada para obtener la información fue la encuesta, la misma facilitó la recolección en forma directa a fin de diagnosticar como es la seguridad de la información en la Unexpo, Vicerrectorado Puerto Ordaz. En

este sentido, Hernández, R. y otros 2003, señala que una técnica es un procedimiento más o menos estandarizado que se ha utilizado con éxito en el ámbito de la ciencia. Asimismo, indica que el instrumento de recolección de datos es un dispositivo de sustrato material que sirve para registrar los datos obtenidos a través de las diferentes fuentes.

Para recabar la información se elaboró el instrumento en función de los objetivos definidos en el presente estudio, con el propósito de interrogar a los sujetos de estudios, a través de .un cuestionario estructurado con preguntas cerradas. Al respecto, los autores, señalan que un cuestionario consiste en "Un conjunto de preguntas respecto a una o más variables a medir relacionadas con los indicadores que se obtienen de la operacionalización de los objetivos específicos." (p. 285). El cuestionario constará de sesenta y nueve (69) ítems (Ver anexo C), con opciones de respuestas en un formato de escala tipo Likert; Siempre (S), Casi Siempre (CS) Algunas veces (AV), Casi Nunca (CN) y Nunca (N), con el fin de diagnosticar cómo es la seguridad de la información en la universidad. Las preguntas cubren todos los aspectos de riesgos, incluso las amenazas a la confiabilidad, integridad y la disponibilidad de los datos y están basadas en los objetivos de control de la ISO 27001:2005: a) Políticas de seguridad, b) Organización de la Seguridad de la Información, c) Gestión de activos, d) Seguridad de recursos humanos, e) Seguridad física y Ambiental, f) Gestión de comunicaciones y operaciones, g) Control de Accesos, h) Adquisición, desarrollo y mantenimiento de sistemas de información, i) Gestión de incidente de seguridad de la información, j) Gestión de continuidad del negocio y k) Cumplimiento.

Dada la naturaleza del estudio y en función de los datos que se requieren, se utilizó la técnica de observación directa, no participante y sistemática en la realidad. Al respecto, Hurtado (1998), indica que "la observación consiste en el registro sistemático, válido y confiable de comportamiento" (p.74). Cuando se habla de observación no participativa, se refiere a que "el investigador asumirá un papel de espectador de los hechos, del conjunto de actividades y relaciones

laborales que se producen cotidianamente" (p.75) y cuando se refiere al término sistemático, la autora indica que "se observa todo lo relativo a los antecedentes, forma, duración y frecuencia en que se originan los mismos".

### *Validez del Instrumento*

De acuerdo a Balestrini (ob.cit.), la validez es un concepto del cual pueden tenerse diferentes tipos de evidencias relacionadas con el contenido, criterio y con el constructo. En este sentido, la validez de contenido se refiere al grado en que un instrumento refleja un dominio específico de contenido de lo que se mide. La autora señala que "Es el grado en que la medición representa al concepto medido" (p.83).

De igual manera, la autora anteriormente citada señala que la validez de criterio establece la validez de un instrumento de medición comparándola con algún criterio externo, que es un estándar con el que se juzga la validez del instrumento, considerándose que entre más se relacionen los resultados del instrumento de medición con el criterio, la validez del criterio será mayor. Asimismo, la validez de constructo se refiere al grado en que una medición se relaciona consistentemente con otras, de acuerdo con hipótesis derivadas teóricamente sobre esa variable, siendo un constructo una variable medida dentro de una teoría o esquema teórico.

Para determinar la validez del instrumento se utilizó la técnica de juicio de expertos, donde se eligieron tres especialistas, profesores universitarios con grado de Magíster, versados en el tema, quienes a través de un formato de validación (Anexo D), todo esto se hizo con la finalidad de modificar la redacción de los ítems, en caso necesario y así determinar la existencia o no de ambigüedad en la redacción de los mismo, buscando la mayor claridad, congruencia y pertinencia posible. Luego de las correcciones y recomendaciones del caso se procedió a la elaboración del instrumento definitivo a ser aplicado a los sujetos de la muestra.

*Confiabilidad del Instrumento*

Hernández, S. y otros (ob. cit.), consideran que la confiabilidad de un instrumento de medición, es la "capacidad que tiene de registrar los mismos resultados en repetidas ocasiones, con una misma muestra y bajo las mismas condiciones" (p.123).

La confiabilidad del instrumento se determinó previa aplicación de prueba piloto a un grupo de diez (10) personas, tomados al azar perteneciente a la Oficina Regional de Tecnología y Servicios de Información y a los diferentes departamentos y unidades administrativas donde están los módulos de Sistema Administrativo Integrado SAI, todos ellos con características similares a los sujetos de estudio. Los resultados obtenidos se procesaron estadísticamente mediante el método Alpha de Cronbach, el cual según lo expresado por Ruiz (1998), es el método que más se adapta en los casos de la medición de constructos a través de escalas, allí no existen respuestas correctas ni incorrectas, el sujeto marca el valor de la escala que considera representa mejor su punto de vista. El coeficiente Alpha de Cronbach, indica la capacidad que tiene el instrumento para arrojar resultados similares en repetidas ocasiones. Para determinarlo se empleo la siguiente formula:

$$\alpha = \left( \frac{N}{N-1} \right) * \left( 1 - \frac{\Sigma SI^2}{St^2} \right)$$

En donde:

N = Es el numero de ítems.

$\Sigma$ $SI^2$ = Sumatoria de la varianza por ítems.

$St^2$ = Varianza Total.

El índice de confiabilidad debe ser menor o igual a uno (1) para que el valor indicativo del instrumento posea un alto grado de consistencia interna, lo que indica la exactitud y objetividad en los resultados.

Los criterios establecidos para el análisis del coeficiente de Alpha de Cronbach, según Hernández y otros (ob.cit.) son los siguientes:

**Cuadro 3**

**Criterios de Confiabilidad**

| Valores de Alpha | Criterios |
|---|---|
| De –1 a 0 | No es confiable |
| De 0.01 a 0.49 | Baja confiabilidad |
| De 0.50 a 0. 75 | Moderada confiabilidad |
| De 0.76 a 0.89 | Fuerte confiabilidad |
| De 0.90 a 1.00 | Alta confiabilidad |

Fuente: Metodología de la Investigación, por Hernández et al (2003)

Luego de aplicar el método Alpha de Cronbach (Anexo E), se obtuvo una confiabilidad de 0,96, lo cual indicó que es altamente confiable.

*Técnicas de Análisis de los Datos*

Una vez que se obtenidos los resultados, producto de la aplicación del instrumento se procedió a su ordenación para analizarlos mediante la estadística descriptiva, que Hurtado (ob.cit.), señala como “el uso de bases estadísticas de frecuencias y porcentajes; complementados con cuadros y gráficos estadísticos con sus respectivos análisis” (p.52).

*Resultados*

Seguidamente se presenta los resultados de la aplicación del cuestionario dirigido al personal técnico y usuario de Sistema Administrativo Integrado SAI, de los módulos de presupuesto, compra, tesorería, contabilidad y almacén del Vicerrectorado de Puerto Ordaz, fue tabulada manualmente, según las

categorías de respuestas: S = Siempre, CS = Casi Siempre, AV = Algunas Veces, CN = Casi Nunca y N = Nunca, según lo establecido por escalamiento líkert el valor uno (1) es asignado a N (Nunca) y el máximo valor de cinco (5) a S (Siempre).

Para presentar los resultados se usaron los recursos de la estadística descriptiva que permitió el diseñó de los cuadros, donde se organizaron los datos recabados en distribuciones por frecuencias absolutas y luego a porcentajes, se representó gráficamente mediante diagramas de barras cada una de las preguntas del instrumento de recolección de datos.

Con el objeto de visualizar en forma rápida los resultados se agruparon con relación a las dimensiones señaladas en la definición operacional de los aspectos a investigar y representados gráficamente de acuerdo a las alternativas seleccionadas.

Posteriormente, se completó este proceso con un análisis e interpretación de los datos en función de la norma ISO/IEC 27001:2005 y las bases teóricas que sustentaron la investigación.

**Dimensión:** Política de Seguridad.

Esta dimensión contiene tres (3) ítems que permitieron obtener información si en la Unexpo dan soporte a la gestión de la seguridad de la información de acuerdo a los requisitos de la universidad, las leyes y reglamentos existentes.

**Cuadro 4**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Políticas de Seguridad.

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3,85 | 2 | 6,90 | 3 | 11,54 | 6 | 23,08 | 14 | 53,85 |
| 2 | 2 | 7,69 | 6 | 20,69 | 7 | 26,92 | 7 | 26,92 | 4 | 15,38 |
| 3 | 0 | 0,00 | 2 | 6,90 | 2 | 7,69 | 11 | 42,31 | 11 | 42,31 |

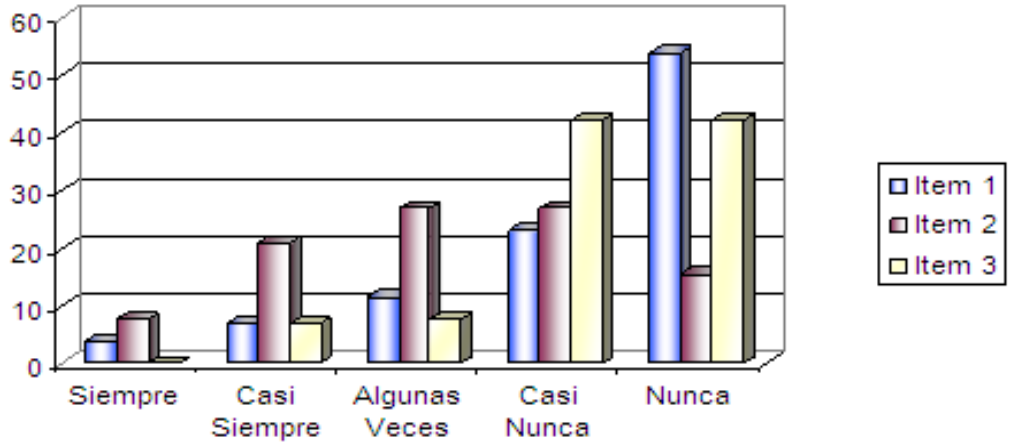



**Gráfico 1**. Porcentajes de las respuestas dadas a las preguntas sobre Políticas de Seguridad.

De acuerdo a las respuestas emitidas de los sujetos en estudio y el análisis e interpretación de las mismas, se puede visualizar en el cuadro 4 y gráfico 1 referido a la dimensión: Políticas de Seguridad, en el ítem 1: (¿Existe una preocupación dentro de la Unexpo por la elaboración de un documento de políticas de seguridad de información con los procedimientos a seguir para cada uno de los riesgos más graves que tiene la información? ) la mayor tendencia porcentual se presentó en la alternativa nunca con un 53,85%, lo cual indica que no existe una preocupación por elaborar un documento de política de seguridad de la información.

En el ítem 2, (¿Se toman acciones rápidas y correctivas cuando la información está en riesgo?), un 26, 92% piensa que Algunas Veces o Casi Nunca lo hacen, esto refleja que no se tiene una consciencia de la importancia de tomar medidas para proteger la información. Igualmente, en el Ítem 3, (¿Se revisan periódicamente las medidas y procedimientos de seguridad para determinar si son efectivos?), la mayor tendencia con un 42,31% se presentó para las alternativas Casi Nunca y Nunca, es evidente que no existe una política clara en referencia a la seguridad de la información.

En conclusión, para poder dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos de la universidad, se deben realizar dos documentos para considerar la seguridad de la información: el primero será un manual de política de seguridad de la información que representará el nivel político o estratégico de la Unexpo, deberá ser aprobado por Consejo Universitario, lo cual como la mayor línea rectora, definirá las grandes líneas a seguir y el nivel de compromiso de la universidad con ellas y el segundo documento será el plan de seguridad, como nivel de planeamiento o táctico, el cual definirá el "Cómo". Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones o líneas rectoras que se deberán cumplir. Es de destacar que una "Política de Seguridad" bien planteada, diseñada, y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero Sistema de Gestión de Seguridad de la Información (SGSI).

**Dimensión:** Organización de la Seguridad de la Información

Esta dimensión contiene siete (7) ítems que permitieron obtener información sobre la manera de accesar, procesar, comunicar o gestionar la seguridad de la información tanto dentro de la universidad como con las partes externas.

**Cuadro 5**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Organización de la Seguridad de la Información

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 0 | 0,00 | 0 | 0,00 | 5 | 19,23 | 13 | 50,00 | 8 | 30,77 |
| 5 | 0 | 0,00 | 1 | 3,85 | 6 | 23,08 | 11 | 42,31 | 8 | 30,77 |
| 6 | 0 | 0,00 | 1 | 3,85 | 8 | 30,77 | 10 | 38,46 | 7 | 26,92 |
| 7 | 2 | 7,69 | 1 | 3,85 | 7 | 26,92 | 11 | 42,31 | 5 | 19,23 |
| 8 | 1 | 3,85 | 0 | 0,00 | 4 | 15,38 | 15 | 57,69 | 6 | 23,08 |
| 9 | 0 | 0,00 | 1 | 3,85 | 5 | 19,23 | 8 | 30,77 | 12 | 46,15 |
| 10 | 1 | 3,85 | 6 | 23,08 | 10 | 38,46 | 5 | 19,23 | 4 | 15,38 |

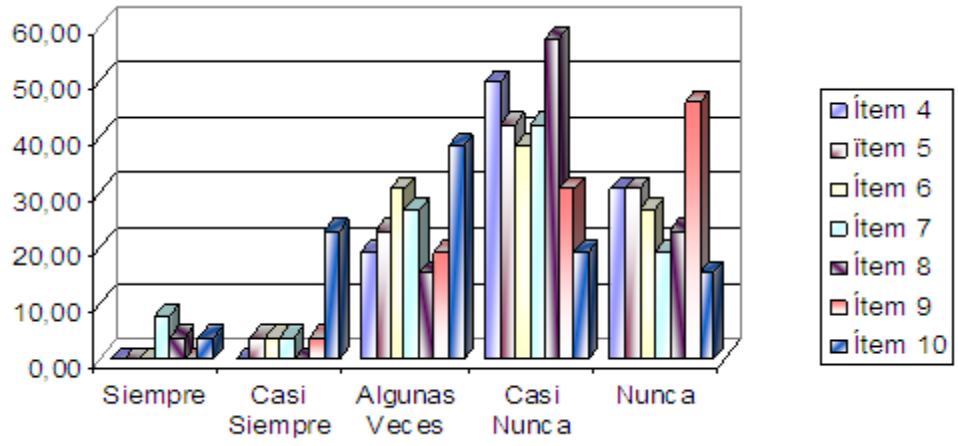



**Gráfico 2**. Porcentajes de las respuestas dadas a las preguntas sobre Organización de la Seguridad de la Información.

En el cuadro 5 y grafico 2, se observan los resultados obtenidos en cuanto a la dimensión organización de la seguridad de la información, en el item 4 (¿El Vicerrector regional y los jefes de las diferentes unidades administrativas del Vicerrectorado de Puerto Ordaz entienden, apoyan y llevan a cabo eficazmente políticas de seguridad de la información dentro la Universidad?), el 50% respondió Casi Nunca y un 30,77 Nunca. Igualmente en los ítem 5 (¿La Unexpo se preocupa de que el personal tome consciencia sobre la importancia de la seguridad de la información y sus responsabilidades individuales para alcanzarla?) e ítem 6 (¿Se definen claramente todas las responsabilidades en torno a la seguridad de la información?) los resultados presentaron la mayor tendencia hacia Casi Nunca y Nunca, lo que permite determinar que no existe un compromiso demostrado, por parte de las autoridades regionales y los diferentes jefes de departamentos y unidades administrativa, asi como tampoco el reconocimiento de las responsabilidades de seguridad de la información.

En el item 7, (¿Se define e implementa un proceso de autorización para los recursos de procesamiento de la información?), el 42,31% opinó Casi Nunca y un 26,92% Algunas Veces, lo que permite establecer que no se tiene claramente definidos los proceso de autorización para cada nuevo recurso de

procesamiento de la información. Seguidamente, el item 8 permitió indagar sobre los acuerdos de confidencialidad o no divulgación de la información y el mayor porcentaje lo presentó la alternativa Casi Nunca con un 57,69%, es evidente que se deben identificar los requisitos para los acuerdos de no divulgación de la información para proteger la información de carácter institucional y privada de la universidad.

En el item 9 (¿Se tienen previstos mecanismos de seguridad para preservar la información de intervenciones externas?), el 46,15% manifestó que Nunca, se puede inferir que no estan identificados los riesgos a la información de la Universidad y en consecuencia no están implementados los controles apropiados antes de otorgar el acceso a partes externas. En el item 10 (¿Se consideran todos los requisitos de seguridad identificados antes de dar el acceso al cliente o usuario a la información o posesiones de la universidad?), el 38,46 % respondió que Algunas Veces, mientras que el 23.02% piensa que Casi Siempre se tratan todos los requisitos de seguridad antes de dar el acceso al cliente o usuario de la información.

En conclusión, existe una alta tendencia en todos los ítems hacia la alternativa Casi Nunca, los sujetos de estudios señalan que en la universidad no se llevan eficazmente las políticas de seguridad de la información y no están definidas claramente todas las responsabilidades individuales para alcanzarla. Igualmente, no está definido los requisitos para los acuerdos de confidencialidad de la información, ni se consideran todos los requisitos de seguridad antes de dar acceso al cliente o usuario de la información externo a la universidad.

**Dimensión:** Gestión de Activos.

Este indicador contiene cuatro (4) ítems que permitieron obtener información referente si se mantiene la protección apropiada de los activos de la universidad.

**Cuadro 6**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Gestión de Activos.

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 3 | 11,54 | 2 | 7,69 | 13 | 50,00 | 8 | 30,77 | 0 | 0,00 |
| 12 | 20 | 76,92 | 4 | 15,38 | 2 | 7,69 | 0 | 0,00 | 0 | 0,00 |
| 13 | 6 | 23,08 | 16 | 61,54 | 2 | 7,69 | 1 | 3,85 | 1 | 3,85 |
| 14 | 0 | 0,00 | 1 | 3,85 | 2 | 7,69 | 19 | 73,08 | 4 | 15,38 |

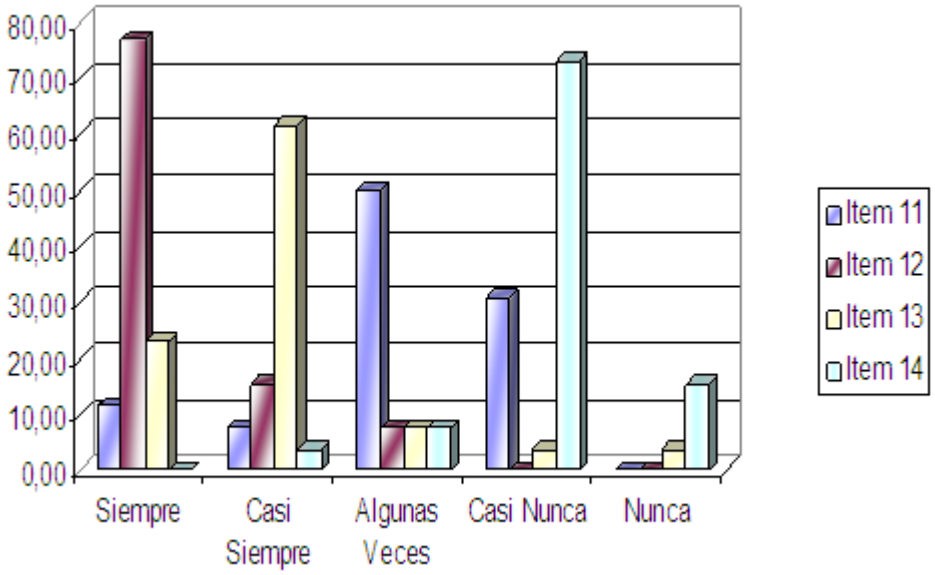



**Gráfico 3**. Porcentajes de las respuestas dadas a las preguntas sobre Gestión de Activos.

Los resultados obtenidos en la dimensión gestión de activos se expresados en el Cuadro 6 y el gráfico 3, en el ítem 11 (¿Se identifican los equipos de computación, tales como: laptops, computadoras de escritorio y otros, con el nombre de la Universidad, nombre del departamento u oficina, teléfono, serial del equipo, serial de bienes nacionales, entre otros?), el 50% opinó Algunas Veces y un 30,77% señaló Casi Nunca, esto refleja que no todos los activos estan identificados lo que ocasiona que los inventarios no estan actualizados, lo

cual es indispensable para el sistema de información SAI, para el módulo de Bienes Nacionales que aún no está en producción.

En el ítem 12 (¿Se realizan inventarios en cada oficina o unidad administrativa de los equipos informáticos y de comunicaciones, con el serial del equipo, software instalados, usuario asignado, ubicación, entre otros?), el 76,92% opino que Siempre se realizan los inventarios.

Igualmente, el ítem 13 (¿Se identifican todos los activos de información para conocer su contenido y a qué departamento pertenecen?), el 61,54% señaló que Casi Siempre. Es de destacar, que existen inventarios de equipos infórmaticos y los activos están identificados, en los diferentes departamentos y unidades administrativas donde opera los módulos del SAI.

El ítem 14 (¿Se dan directrices para clasificar la información de acuerdo con su valor, requisitos legales, sensibilidad y criticidad para la universidad?), el 73,08% opinó que que Casi Nunca se dan directrices, lo que refleja que la información está inventariada y clasificada pero no existe un procedimiento con un esquema de clasificación establecido para etiquetar los activos de información.

En conclusión: En el Vicerrectorado de Puerto Ordaz se cuenta con un departamento de Bienes Nacionales el cual es el encargado de realizar el inventario de todos los activos importantes, sin embargo, según el resultado de la encuesta el mismo esta desactualizado, ya que no se sabe fehacientemente lo que se posee y existen activos que aún no han sido inventariados, lo cual es un hueco de seguridad de todo el sistema. Es evidente que se debe tener una metodología para realizar esta actividad donde cada activo de información este asociado con el lugar donde se procesa la información y que a su vez sea el responsable por el mismo.

**Dimensión:** Seguridad de Recursos Humanos.

Esta dimensión contiene cinco (5) ítems que permitieron obtener información si los empleados, contratistas y usuarios del sistema administrativo

integrado SAI antes y durante el empleo comprenden sus responsabilidades, si están concientes de las amenazas de la seguridad de la información a fin de reducir el riesgo del robo, fraude o mal uso de los recursos de la universidad. Igualmente, al terminar o cambiar de lugar de trabajo se retiran o cambian de una manera ordenada.

**Cuadro 7**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Seguridad de Recursos Humanos.

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 0 | 0,00 | 0 | 0,00 | 10 | 38,46 | 15 | 57,69 | 1 | 3,85 |
| 16 | 0 | 0,00 | 0 | 0,00 | 6 | 23,08 | 18 | 69,23 | 2 | 7,69 |
| 17 | 1 | 3,85 | 1 | 3,85 | 2 | 7,69 | 14 | 53,85 | 8 | 30,77 |
| 18 | 1 | 3,85 | 6 | 23,08 | 14 | 53,85 | 4 | 15,38 | 1 | 3,85 |
| 19 | 3 | 11,54 | 1 | 3,85 | 16 | 61,54 | 3 | 11,54 | 3 | 11,54 |

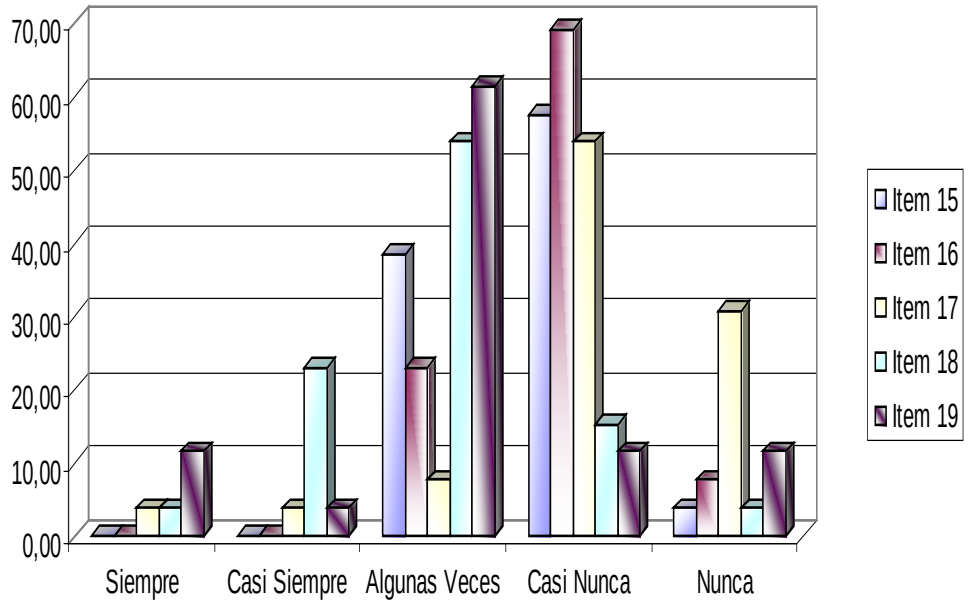



**Gráfico 4**. Porcentajes de las respuestas dadas a las preguntas sobre Seguridad de Recursos Humanos.

En el cuadro 7 y gráfico 4, se visualizan los resultados de la dimensión seguridad de recursos humanos. Al respecto, el ítem 15 (¿Se realiza una verificación de los antecedentes de los candidatos para ocupar cargos administrativos, contratistas y usuarios de terceras partes de acuerdo con las leyes, reglamentaciones y ética pertinentes a los requisitos de la Universidad, clasificación de información a ser accesada y los riesgos percibidos? ), la mayor incidencia de respuesta la presentó la alternativa Casi Nunca con un 57,69%, mientras que el 38,46% opinó que Algunas Veces, lo que permite inferir que se realiza una verificación de los documentos suministrados por el aspirante pero no sus antecedentes para poder optar al cargo de acuerdo con las responsabilidades que desempeñará.

En el ítem 16 (¿La Universidad aplica procesos disciplinarios a los funcionarios que cometan un incumplimiento de seguridad?) y el ítem 17 (¿Se vigilan la moral y el comportamiento del personal que maneja los sistemas de información con el fin de mantener una buena imagen y evitar un posible fraude?), presentaron su mayores incidencia en la alternativa Casi nunca con un 69,23% y 53,85% respectivamente, lo que evidencia que no existe un proceso disciplinario formal para los funcionarios que incurran en faltas que atente a la seguridad de la información, igualmente no se realizan supervisiones a los funcionarios para evitar posibles fraudes.

En referencia a la devolución de los activos, el ítem 18 (¿Se retiran los derechos de acceso a todos los empleados, contratistas y usuarios de terceras partes a la información y al recurso para el procesamiento de la información una vez terminado su empleo, contrato o acuerdo, o una vez ajustado el cambio a otra dependencia?) y el ítem 19 (¿La Universidad se asegura de que los empleados, contratista y usuarios de terceras partes devuelvan todos los activos de la Universidad que posean una vez terminado su empleo, contrato o acuerdo?) los sujetos de estudios coincidieron que la alternativa que mas se ajustó fue Algunas Veces presentando un 53,85% y 61,54% respectivamente, lo que demuestra que no está establecido un procedimiento para la devolución de

todos los activos de la universidad y no toman las debidas previsiones para retirar todos los derechos de accesos a la información.

Es de destacar, que esta dimensión se debe trabajar en conjunto tanto el Departamento de Personal y el encargado de la seguridad y control de la Oficina Regional de Tecnología y Servicios de Información, en la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos (por solicitud, cambio o despido). En la misma deberá quedar bien claro las acciones a seguir para los diferentes perfiles de la universidad, basados en la responsabilidad de manejo de información que tenga ese puesto. Como se puede apreciar, tanto la contratación como el cese de un puesto, es una actividad conjunta de estas dos áreas, y cada paso deberá ser coordinado, según la documentación confeccionada, para que no se pueda pasar por alto ningún detalle, pues son justamente estas pequeñas omisiones de las que luego resulta el haber quedado con alta dependencia técnica de personas cuyo perfil es peligroso, o que al tiempo de haberse ido, mantiene accesos o permisos que no se debieran (casos muy comunes).

**Dimensión:** Seguridad Física y Ambiental.

Esta dimensión contiene quince (15) ítems que permitieron obtener información en relación al área de seguridad: Seguridad física y perimetral, control físico de entradas, seguridad de las oficinas, edificios y recursos, protección contra amenazas externas y del entorno, así como también a la seguridad de los equipos: ubicación y protección de equipos, elementos de soporte a los equipos, seguridad en el cableado, mantenimiento de equipos, seguridad en el equipamiento fuera de la organización, seguridad en la redistribución o reutilización de equipamiento, borrado de información y/o software.

**Cuadro 8**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Seguridad Física y Ambiental.

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 20 | 0 | 0,00 | 2 | 7,69 | 2 | 7,69 | 2 | 7,69 | 20 | 76,92 |
| 21 | 0 | 0,00 | 1 | 3,85 | 1 | 3,85 | 7 | 26,92 | 17 | 65,38 |
| 22 | 0 | 0,00 | 0 | 0,00 | 0 | 0,00 | 7 | 26,92 | 19 | 73,08 |
| 23 | 0 | 0,00 | 1 | 3,85 | 4 | 15,38 | 7 | 26,92 | 14 | 53,85 |
| 24 | 9 | 34,62 | 12 | 46,15 | 3 | 11,54 | 1 | 3,85 | 1 | 3,85 |
| 25 | 7 | 26,92 | 14 | 53,85 | 1 | 3,85 | 2 | 7,69 | 2 | 7,69 |
| 26 | 0 | 0,00 | 0 | 0,00 | 1 | 3,85 | 2 | 7,69 | 23 | 88,46 |
| 27 | 0 | 0,00 | 0 | 0,00 | 1 | 3,85 | 1 | 3,85 | 21 | 80,77 |
| 28 | 0 | 0,00 | 0 | 0,00 | 2 | 7,69 | 5 | 19,23 | 19 | 73,08 |
| 29 | 1 | 3,85 | 1 | 3,85 | 3 | 11,54 | 7 | 26,92 | 14 | 53,85 |
| 30 | 2 | 7,69 | 2 | 7,69 | 4 | 15,38 | 10 | 38,46 | 8 | 30,77 |
| 31 | 0 | 0,00 | 0 | 0,00 | 1 | 3,85 | 4 | 15,38 | 21 | 80,77 |
| 32 | 1 | 3,85 | 7 | 26,92 | 14 | 53,85 | 2 | 7,69 | 2 | 7,69 |
| 33 | 0 | 0,00 | 0 | 0,00 | 7 | 26,92 | 7 | 26,92 | 12 | 46,15 |
| 34 | 2 | 7,69 | 3 | 11,54 | 8 | 30,77 | 7 | 26,92 | 6 | 23,08 |

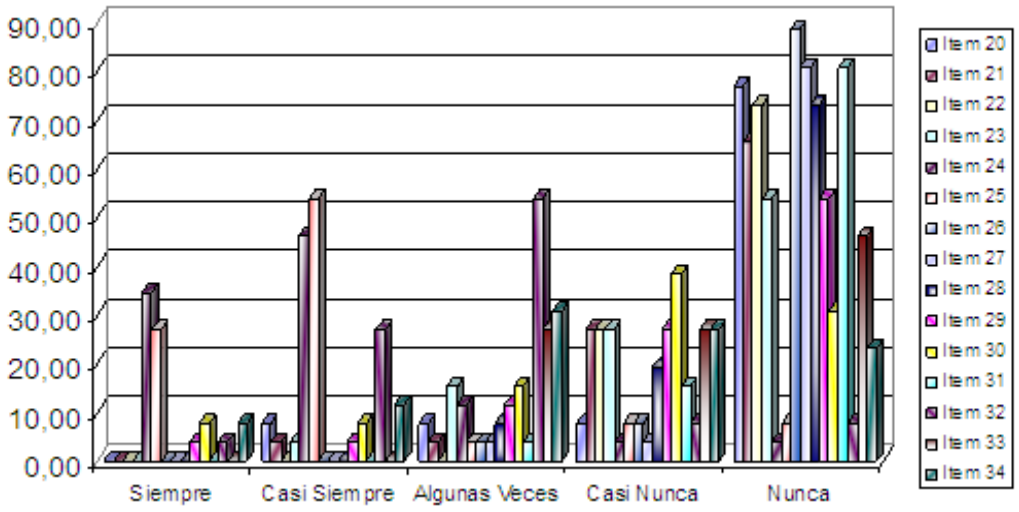



**Gráfico 5**. Porcentajes de las respuestas dadas a las preguntas sobre Seguridad Física y Ambiental.

El cuadro 8 y grafico 5, muestra los resultados aportados por los sujetos de estudios en relación a la seguridad física y ambiental. En este sentido, los ítems 20 (¿En la Universidad se establecen adecuadamente los perímetros de

seguridad (barreras tales cómo paredes, puertas de entradas controladas por tarjetas o puesto de recepción manual) a las áreas que contienen la información y las instalaciones de procesamiento de la información?), ítem 21 (¿Se diseñan y aplican controles de entradas apropiados a las áreas de seguridad a fin de asegurar el permiso de acceso sólo al personal autorizado?, ítem 22 (¿Existe un procedimiento o control de admisión al edificio administrativo para aquellas personas que no posean carnet institucional, tal como los visitantes?) e ítem 23 (¿Se controla el ingreso a las oficinas después del horario normal de trabajo?), presentan una alta tendencia a la alternativa Nunca, lo que permite inferir que no están establecido los perímetros de seguridad para las áreas que contienen información critica de la universidad, como por ejemplo la sala principal de cableado y de servidores. Igualmente, no se cumplen procedimientos para permitir el acceso solo al personal autorizado.

En lo que respecta a los controles físicos de entrada, el ítem 24 (¿Se cierran con llave las puertas de los sitios neurálgicos en el edificio administrativo?) e ítem 25 (¿Se cierran con llaves las entradas de cada piso, asi cómo las entradas externas al edificio administrativo?), las alternativas con mayor porcentajes se observan en Casi Siempre con 46,15% y 53,85% respectivamente, lo que refleja cierta dudas de los sujetos de estudios para responder si se cumple o no el mantener las puertas de entradas cerradas para impedir el paso de personal no autorizado sobre todo fuera del horario de oficina.

En relación a la protección contra las amenazas externas y ambientales, se formularon las siguientes preguntas, ítem 26. ¿Se diseñan y aplican protección física a las oficinas contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre? e ítem 27. ¿Se diseñan y aplican protección física a la información contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre?, las respuestas estuvieron orientadas con un 88,46% y un 80,77% respectivamente a la alternativa Nunca, reflejando que la

Unexpo no ha considerado la protección física tanto a las oficinas como a la información contra los desastres naturales o provocados por el hombre.

Para indagar sobre la ubicación y protección de los equipos, el ítem 28. ¿La Universidad toma medidas concretas para evitar el robo de equipos tales como laptops y otros componentes? y el ítem 29. ¿Se toman previsiones de ubicar o proteger los equipos para reducir los riesgos de amenazas y peligros ambientales, y oportunidades para el acceso no autorizado?, los resultados indican una tendencia negativa hacia las alternativas Casi Nunca y Nunca, esto demuestra la poco preocupación manifestadas en la universidad por prevenir pérdidas, daños o robo de los activos de información.

El ítem 30 (¿Se protegen los equipos contra fallas de energía y otras interrupciones eléctricas causadas por problemas en los servicios de apoyo?), la alternativa Casi Siempre presentó un 38,46%, Nunca un 30,77%, Algunas Veces 15,38% y las alternativas Siempre y Casi Siempre un 7,69%, estos resultados no son concluyentes lo permite inferir que los sujetos encuestados desconocen sobre las medidas que se deben considerar para proteger los equipos contra las fallas de energía u otras interrupciones electricas.

El ítem 31 (¿Se protegen debidamente el cableado de energía eléctrica y de comunicaciones que transporta datos contra la interceptación o daños?), el 80,77% respondió que Nunca evidenciando una grave falla en la seguridad del cableado. El ítem 32 (¿Se realizan mantenimientos preventivos a los equipos a fin de asegurar su continua disponibilidad e integridad?), el 53,85% opinó que Algunas Veces se realizan mantenimientos a los equipos.

El ítem 33 (¿Se toman las previsiones para que todos los dispositivos de almacenamiento de datos (flash memory o pendrive, CD, Disquette, Disco duros, entre otros), sean eliminados o formateado completamente ante de su disposición?), el 46,25% se inclinó por la alternativa Nunca y el 26,92% Casi Nunca evidenciando huecos o vacios en la seguridad de la información cuando se reutizan o eliminan equipos sin tomar las previsiones de remover toda la información existentes en el mismo.

El ítem 34 (¿La Unexpo da instrucciones claras y firmes a los vigilantes para que prohiban el traslado o retiro de equipo, información o software sin autorización?), el 30,77 opinó que Algunas Veces mientras que el 26,92% indicó que Casi Nunca, estos resultados evidencia que no existe una política de seguridad que controle el retiro de los activos de información de la universidad.

En conclusión, los resultados mostrados anteriormente demuestran que existen fallas graves en la universidad especificamente en las oficinas donde el sistema administrativo integrado SAI se encuentra en producción para garantizar la seguridad física tanto a las instalaciones como a los equipos. En este sentido, Corletti, (2006) señala que para obtener los mejores resultados de una infraestructura de seguridad de la información, está deberá ser planteada utilizando el modelo OSI, o al modelo TCP/IP, para lograr dividir bien la tarea.

**Dimensión:** Gestión de Comunicaciones y Operaciones.

Esta dimensión contiene catorce (14) ítems que permitieron obtener información sobre la forma de operación de los recursos de información.

**Cuadro 9**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Gestión de Comunicaciones y Operaciones.

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 35 | 0 | 0,00 | 1 | 3,85 | 5 | 19,23 | 15 | 57,69 | 5 | 19,23 |
| 36 | 1 | 3,85 | 1 | 3,85 | 3 | 11,54 | 17 | 65,38 | 4 | 15,38 |
| 37 | 0 | 0,00 | 1 | 3,85 | 7 | 26,92 | 13 | 50,00 | 5 | 19,23 |
| 38 | 2 | 7,69 | 2 | 7,69 | 9 | 34,62 | 7 | 26,92 | 6 | 23,08 |
| 39 | 0 | 0,00 | 4 | 15,38 | 8 | 30,77 | 7 | 26,92 | 7 | 26,92 |
| 40 | 0 | 0,00 | 0 | 0,00 | 2 | 7,69 | 14 | 53,85 | 10 | 38,46 |
| 41 | 0 | 0,00 | 15 | 57,69 | 2 | 7,69 | 3 | 11,54 | 6 | 23,08 |
| 42 | 1 | 3,85 | 3 | 11,54 | 3 | 11,54 | 11 | 42,31 | 8 | 30,77 |
| 43 | 2 | 7,69 | 2 | 7,69 | 5 | 19,23 | 7 | 26,92 | 10 | 38,46 |
| 44 | 1 | 3,85 | 2 | 7,69 | 2 | 7,69 | 14 | 53,85 | 7 | 26,92 |
| 45 | 0 | 0,00 | 0 | 0,00 | 4 | 15,38 | 16 | 61,54 | 6 | 23,08 |
| 46 | 0 | 0,00 | 0 | 0,00 | 2 | 7,69 | 5 | 19,23 | 19 | 73,08 |
| 47 | 1 | 3,85 | 0 | 0,00 | 2 | 7,69 | 7 | 26,92 | 16 | 61,54 |
| 48 | 1 | 3,85 | 1 | 3,85 | 1 | 3,85 | 11 | 42,31 | 12 | 46,15 |

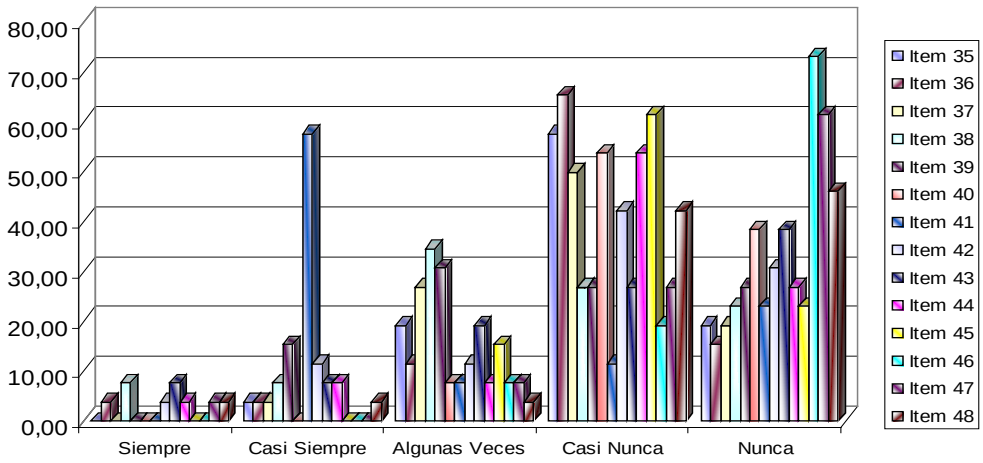



**Gráfico 6**. Porcentajes de las respuestas dadas a las preguntas sobre Gestión de Comunicaciones y Operaciones.

En el cuadro 9 y gráfico 6, se observan los resultados obtenidos para la dimensión gestión de comunicaciones y operaciones. Para indagar sobre los procedimientos y responsabilidades de operación de la información, se emplearon los ítems 35 (¿Los procedimientos operativos son documentados, mantenidos y están disponibles a todos los usuarios que lo necesitan?) y 36 (¿Se controlan los cambios de los recursos y sistemas de procesamiento de la información?), los resultados encontrados tienen una marcada tendencia negativa con un 57,69% y 65,38% en la alternativa Casi Nunca respectivamente, lo que indica que no se realizan mayores esfuerzo por documentar los procedimientos, lo cual es negativo, ya que la documentación de los procedimientos permite el manteniento de los mismos y si estos se encuentran disponibles a todos los usuarios que los necesiten, y se segregan adecuadamente los servicios y las responsabilidades se logra evitar el uso inadecuado de los mismos.

En relación con la planificación y aceptación de los sistemas, el ítem 37, (¿Se realizan seguimientos, ajustes y proyecciones de los requisitos de la capacidad futura de la utilización de los recursos, para garantizar el desempeño

del sistema requerido?), el 50% de los sujetos de estudios opinaron que Casi Nunca se realizan.

Para obtener información sobre la protección contra el código malicioso y movible, se utilizaron los ítem 38 (¿Se implementan controles de detección, prevención y recuperación de la información, para la protección contra código malicioso o virus?) y el ítem 39 (¿Se realizan procedimientos adecuados de toma de conciencia de los usuarios para la detección, prevención y recuperación para la protección contra código malicioso?), las respuestas permitieron concluir que los usuarios tiene poco conocimiento para detectar los códigos maliciosos y no existen procedimientos formales para adiestrarlos para que puedan evitarlos y así proteger la información.

El ítem 40 (¿Se establecen procedimientos para controlar el intercambio de información a través de la utilización de toda clase de recursos de comunicación, por ejemplo el uso de teléfonos celulares y laptops por parte de personas ajenas a la universidad?), el 53,85% opino que Casi Nunca, lo que indican que no existe políticas y procedimientos de intercambio de información.

En relación a las copias de seguridad, el ítem 41 (¿Se controla el acceso a las fotocopiadoras para evitar que se puedan hacer copias de cualquier documento?), el 57,69 % opinó que Casi Siempre se controla y el ítem 42 (¿Se realizan copias de seguridad de la información y software de acuerdo con la política de copia de seguridad acordada?), el 42,31% opinó que Casi nunca, lo que permite inferir que no se realizan backups de la información y de los sistemas de información.

El ítem 43 (¿Se gestionan y controlan adecuadamente la red de datos a fin de protegerla de las amenazas y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la información en tránsito?), el 38,46 % opinó que Nunca y un 26,92% Casi Nunca, lo que hace inferir que no se lleva una buena administración y control de la red, es decir, no se implementan todas las medidas posibles para evitar amenazas y mantener la seguridad de los sistemas y aplicaciones que circula por ella.

En relación de manejo de medios de información, se utilizarón dos (02) ítem para recabar información, el ítem 44 (¿Se tiene el cuidado de no botar información confidencial o vital en las papeleras sin ser destruida previamente? y el ítem 45 (¿Se establecen procedimientos para el manejo y almacenamiento de la información a fin de protegerla contra su uso inadecuado o divulgación no autorizada?), donde la alternativa Casi Nunca presentó los mayores valores con 53,85% y 61,54%, estos resultados señalan que no se toman todas las previsiones para la difusión, modificación, eliminación o destrucción de cualquier elemento capaz de almacenar información (dispositivo USB, CD, discos, cintas, papeles, entre otros tanto fijos como removibles).

El ítem 46 (¿Se producen y mantienen los registros de auditorias cuando se detectan actividades de procesamiento de la información no autorizada, a fin de ayudar a futuras investigaciones y seguimiento de control de accesos?) y el ítem 47 (¿Se registran, analizan y se toman acciones apropiadas cuando se detectan fallas en las actividades y procesamiento de la información no autorizada?), presentaron una alta incidencia en la alternativa Nunca con un 73,08% y un 61,54% respectivamente, estos resultados confirman que no se llevan registros de auditorias de los eventos de seguridad que ocurren en los sistemas de información.

El ítem 48 (¿Se sincronizan los relojes de todos los sistemas de procesamiento de la información pertinentes dentro de la universidad con una fuente de tiempo exacta acordada?), el 46,15% opinó que Nunca y el 42,31% Casi Nunca, lo que evidencia que no se tiene una sincronización de toda la infraestructura de servidores.

**Dimensión:** Control de Accesos.

Esta dimensión contiene seis (06) ítems que permitieron obtener información si se controlan que los usuarios autorizados, acceden únicamente a los recursos sobre los cuales tienen derecho y a ningún otro.

**Cuadro 10**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Control de Accesos.

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 49 | 0 | 0,00 | 2 | 7,69 | 5 | 19,23 | 7 | 26,92 | 12 | 46,15 |
| 50 | 1 | 3,85 | 3 | 11,54 | 3 | 11,54 | 14 | 53,85 | 5 | 19,23 |
| 51 | 0 | 0,00 | 0 | 0,00 | 2 | 7,69 | 17 | 65,38 | 7 | 26,92 |
| 52 | 1 | 3,85 | 1 | 3,85 | 13 | 50,00 | 5 | 19,23 | 6 | 23,08 |
| 53 | 1 | 3,85 | 1 | 3,85 | 3 | 11,54 | 15 | 57,69 | 6 | 23,08 |
| 54 | 0 | 0,00 | 2 | 7,69 | 4 | 15,38 | 17 | 65,38 | 3 | 11,54 |

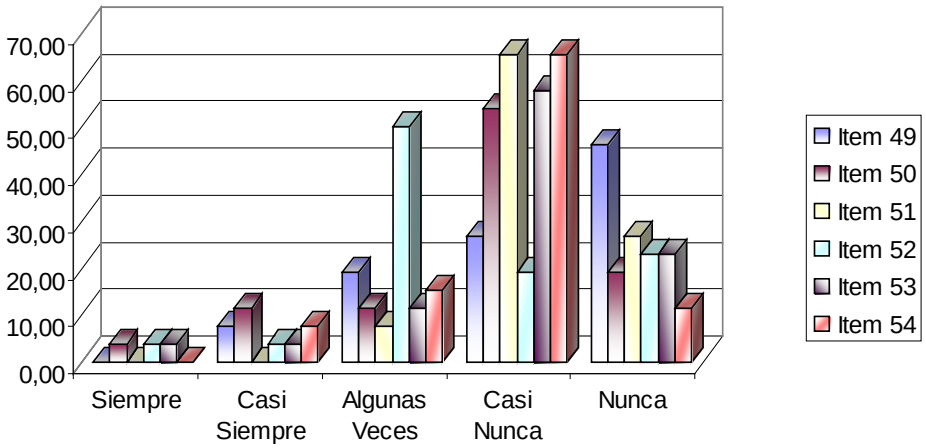



**Gráfico 7**. Porcentajes de las respuestas dadas a las preguntas sobre Control de Accesos.

De acuerdo a las respuestas emitidas de los sujetos en estudio y el análisis e interpretación de las mismas, se puede visualizar en el cuadro 10 y gráfico 7 referido a la dimensión control de accesos, en el ítem 49 (¿Se establecen, documentan y revisan las políticas de control de accesos a la información?), el 46,15% respondió que Nunca, lo cual nos permite inferir que no existe una política de control de accesos.

En relación a la gestión de acceso de usuarios, se emplearon dos preguntas para obtener información, el ítem 50 (¿Se realizan procedimientos formales de registros y des-registros de usuarios para conceder y revocar el

acceso a los sistemas y servicios de información?) y el ítem 51. ¿Se controla a través de un proceso de gestión formal la asignación de contraseñas de usuarios para prevenir el acceso no autorizado a los sistemas de información?), ambas respuestas muestran un alta incidencia por la alternativa Casi Nunca con un 53,85% y un 65,38% respectivamente, lo que nos indica que no existe un procedimiento formal de registro y revocación de usuarios y una adecuada administración de los privilegios y de las contraseñas de cada uno de los usuarios.

En relación al indicador uso de contraseñas el ítem 52 (¿Se le motiva a los usuarios seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas?), el 50% opino que Algunas Veces, esto refleja que los usuarios no tienen claro el uso de contraseñas, así como también evidencia que no existen procedimientos formales para la selección y uso de contraseñas.

El indicador sesión inactiva, el ítem 53 (¿Se activa automáticamente un protector de pantalla protegido con contraseña, cuando el usuario deja de utilizar un tiempo prudencial la máquina?), el 57,69% opino que Casi Nunca, lo que refleja una falla en la seguridad de la información en el momento que un empleado se levante de su puesto y transcurrido un periodo de tiempo prudencial no se apague la sesión da oportunidad a que cualquier persona que no esta autorizado trabaje en el computador, pueda obtener información, cambiarla y hasta borrarla.

El ítem 54 (¿Se restringe de acuerdo con la políticas de control el acceso a la información y a las funciones del sistema de aplicación?) referido al indicador restricción de acceso a la información, el 65,38 respondió que Casi Nunca se hace, esto evidencia que se tiene una política de control de acceso definida.

En conclusión, los resultados obtenidos muestran una inclinación hacia la alternativa Casi Nunca y Nunca. Es de destacar, que el control de acceso es una de las actividades más importantes de la arquitectura de seguridad de un sistema y para lograrlo debe existir una política de control de accesos

documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo. Igualmente, se exige llevar un procedimiento de registro y revocación de usuarios, una adecuada administración de los privilegios y de las contraseñas de cada uno de ellos, realizando periódicas revisiones a intervalos regulares, empleando para todo ello procedimientos formalizados dentro de la universidad.

**Dimensión:** Adquisición, Desarrollo y Mantenimiento de Sistema de Información.

Esta dimensión contiene cinco (05) ítems que permitieron averiguar si la seguridad es una parte integral de los sistemas de información y si se previenen los errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.

**Cuadro 11**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 55 | 2 | 7,69 | 2 | 7,69 | 3 | 11,54 | 4 | 15,38 | 15 | 57,69 |
| 56 | 1 | 3,85 | 3 | 11,54 | 6 | 23,08 | 15 | 57,69 | 1 | 3,85 |
| 57 | 1 | 3,85 | 1 | 3,85 | 3 | 11,54 | 9 | 34,62 | 12 | 46,15 |
| 58 | 0 | 0,00 | 1 | 3,85 | 5 | 19,23 | 14 | 53,85 | 6 | 23,08 |
| 59 | 0 | 0,00 | 1 | 3,85 | 5 | 19,23 | 14 | 53,85 | 6 | 23,08 |

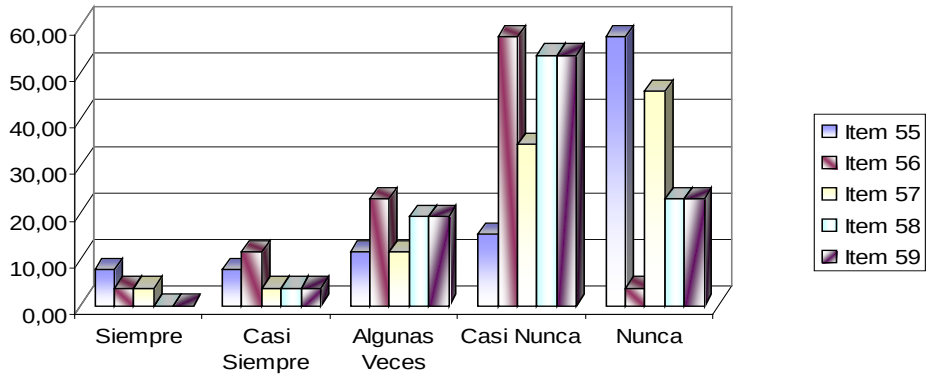



**Gráfico 8**. Porcentajes de las respuestas dadas a las preguntas sobre Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

El cuadro 11 y grafico 8, muestra los resultados aportados por los sujetos de estudios en relación a la adquisición, desarrollo y mantenimiento de sistemas de información. En este sentido, el ítem 55 (¿Se realizan análisis y especificaciones de seguridad para los nuevos sistemas de información o para las mejoras de los sistemas existentes?), el 57,69% opino que Nunca se especifican los requisitos de control de seguridad para los nuevos sistemas de información.

En relación al procesamiento correcto en las aplicaciones, se emplearon tres ítem para obtener información al respecto, el ítem 56 (¿Se realizan validaciones de los datos de entrada a las aplicaciones para asegurarse de que éstos sean correctos y apropiados?), ítem 57 (¿Se incorporan a las aplicaciones las comprobaciones de validación para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados?) y el ítem 58 (¿Se realizan validaciones  a los datos de salida de una aplicación para asegurarse que el procedimiento de la información almacenada es correcto y apropiado a las circunstancias?), los resultados tienen una tendencia negativas observándose los mayores resultados en las alternativas Casi Nunca y Nunca, esto nos permite inferir que no se realiza un correcto tratamiento de la información en las aplicaciones de la universidad, ni se adoptan las medidas para la validación en los datos de entrada, no se tienen controles internos en el procesamiento de al información para verificar o detectar cualquier corrupción de la información a través de los procesos, tanto por error como intencionalmente. Y por último, no existe una validación en la salida de datos, para asegurar que los datos procesados, y su posterior tratamiento o almacenamiento, sea apropiado a los requerimientos de la aplicación.

En el ítem 59 (¿Se desarrollan e implementan políticas sobre la utilización de controles para la protección de confidencialidad, autenticidad o integridad de la información?), el 53,85% opinó que Casi Nunca se protegen la confidencialidad, autenticidad o integridad de la información.

En conclusión, los resultados anteriores demuestran debilidades de seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de información.

**Dimensión:** Gestión de Incidente de Seguridad de la Información

Esta dimensión contiene cuatro (04) ítems que permitieron obtener información si…

**Cuadro 12**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Gestión de Incidente de Seguridad de la Información.

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 60 | 1 | 3,85 | 2 | 7,69 | 4 | 15,38 | 5 | 19,23 | 14 | 53,85 |
| 61 | 2 | 7,69 | 1 | 3,85 | 6 | 23,08 | 14 | 53,85 | 3 | 11,54 |
| 62 | 1 | 3,85 | 0 | 0,00 | 6 | 23,08 | 18 | 69,23 | 1 | 3,85 |
| 63 | 1 | 3,85 | 1 | 3,85 | 3 | 11,54 | 8 | 30,77 | 13 | 50,00 |

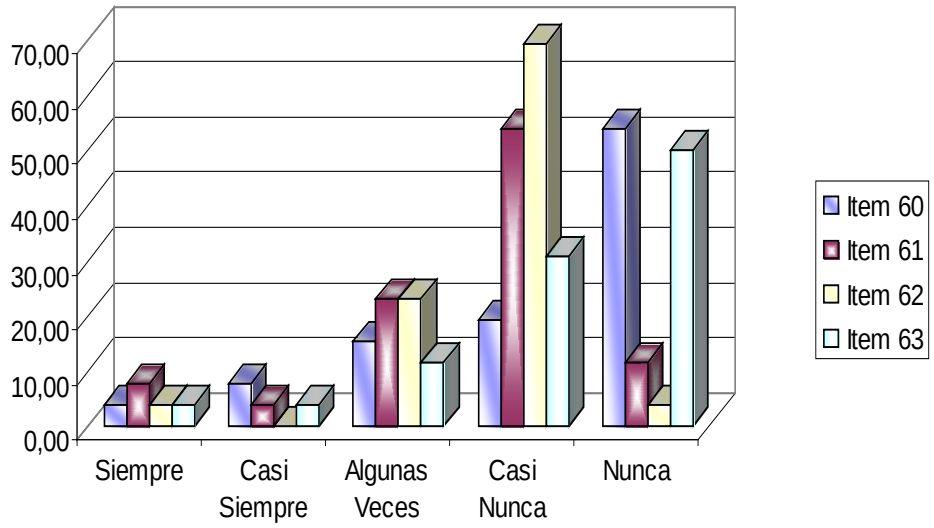



**Gráfico 9**. Porcentajes de las respuestas dadas a las preguntas sobre Gestión de Incidente de Seguridad de la Información.

Los resultados obtenidos en la dimensión gestión de incidentes de seguridad de la información se muestran en el Cuadro 12 y gráfico 9, para obtener información acerca de los reportes de eventos y debilidades de seguridad de la información se emplearon dos preguntas, el ítem 60 (¿Se

reportan los eventos de seguridad de la información a través de los canales de gestión apropiados tan rápidamente cómo sea posible?) y el ítem 61 (¿Se les solicita a todos los usuarios de los sistemas y servicios de información reportar cualquier debilidad en la seguridad de los sistemas o servicios, que haya sido observada o sospechada?), los mayores porcentajes de respuestas un 53,85% fueron para las alternativas Casi Nunca y Nunca, esto refleja que no existen procedimientos para los incidentes de seguridad, por lo contrario se trabaja de manera reactiva, se espera que los eventos sucedan y no se realiza nada por prevenirlos.

En relación a la gestión de los incidentes y mejoras de seguridad de la información, los ítem 62 (¿Se establecen las responsabilidades y procedimiento de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información?) y 63 (¿Se establecen mecanismos que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de seguridad de información?), los resultados señalan un 69,23% opinó que Casi Nunca se establecen responsabilidades y un 50% respondió que Nunca se establecen mecanismos para cuantificar los incidentes de seguridad.

En conclusión, existe una alta tendencia negativa en los resultados, los que demuestra que no se están realizando una administración de los incidentes de seguridad de la información.

**Dimensión:** Gestión de Continuidad del Negocio

Esta dimensión contiene dos (02) ítems que tiene como objetivo contemplar todas las medidas tendientes a que los sistemas de información no hagan sufrir interrupciones sobre la actividad que realiza la universidad.

**Cuadro 13**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Gestión de Continuidad del Negocio

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 64 | 0 | 0,00 | 1 | 3,85 | 18 | 69,23 | 5 | 19,23 | 2 | 7,69 |
| 65 | 1 | 3,85 | 0 | 0,00 | 2 | 7,69 | 4 | 15,38 | 19 | 73,08 |

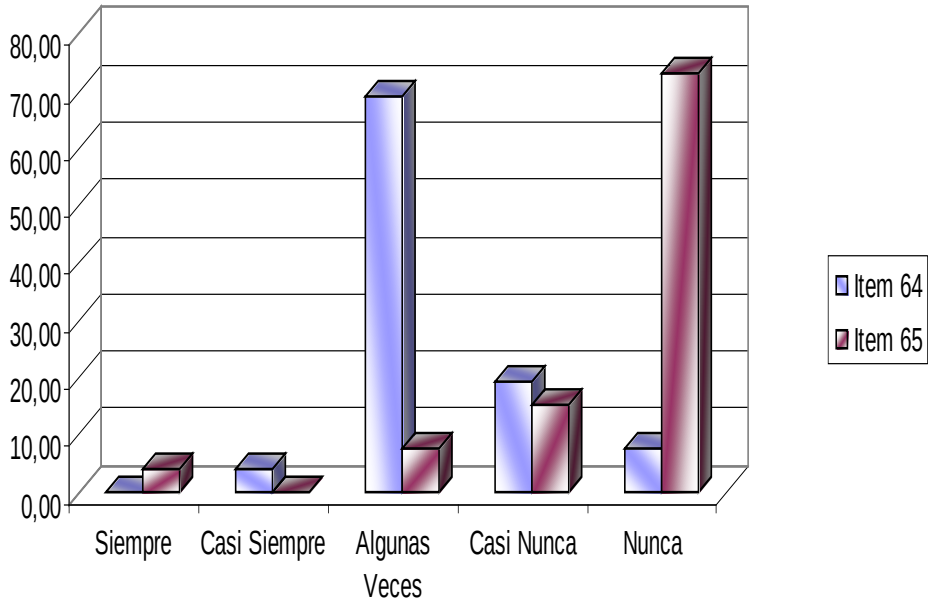



**Gráfico 10**. Porcentajes de las respuestas dadas a las preguntas sobre Gestión de Continuidad del Negocio.

Las respuestas ofrecidas por los usuarios y personal técnico del SAI, visualizadas en el cuadro 13, gráfico 10, permitieron evaluar en relación a la dimensión gestión de continuidad del negocio. En este sentido, el ítem 64 (¿Se identifican los eventos que pueden causar las interrupciones a los procesos de la universidad, al mismo tiempo que la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información?), se observa una tendencia negativa siendo la alternativa Algunas Veces la que presenta mayor puntuación con un 69,23%, esto refleja que no están identificados aquellos eventos que pueden causar interrupción del servicio.

El ítem 65 (¿Se desarrollan e implementan planes para mantener y recuperar las operaciones y asegurar la disponibilidad de la información al nivel requerido y en los plazos requeridos, tras la interrupción o la falla de los procesos críticos de la Universidad?), el 73,08% opinó que Nunca.

Estos resultados evidencian que se tienen poco conocimiento para proteger los procesos administrativos críticos de la universidad de los efectos de fallas significativas de los sistemas de información y asegurar su reanudación oportuna.

**Dimensión:** Cumplimiento

Esta dimensión contiene cuatro (04) ítems que permitieron obtener información si se evitan incumplimientos de cualquier ley, estatuto, obligación reglamentaria o contractual, así como también de cualquier requisito de seguridad.

**Cuadro 14**

Resultados de las respuestas dadas a las preguntas sobre la dimensión Cumplimiento.

| Ítems | S | % | CS | % | AV | % | CN | % | N | % |
|---|---|---|---|---|---|---|---|---|---|---|
| 66 | 0 | 0,00 | 3 | 11,54 | 2 | 7,69 | 14 | 53,85 | 7 | 26,92 |
| 67 | 0 | 0,00 | 3 | 11,54 | 2 | 7,69 | 13 | 50,00 | 8 | 30,77 |
| 68 | 1 | 3,85 | 2 | 7,69 | 9 | 34,62 | 5 | 19,23 | 9 | 34,62 |
| 69 | 0 | 0,00 | 0 | 0,00 | 4 | 15,38 | 9 | 34,62 | 13 | 50,00 |

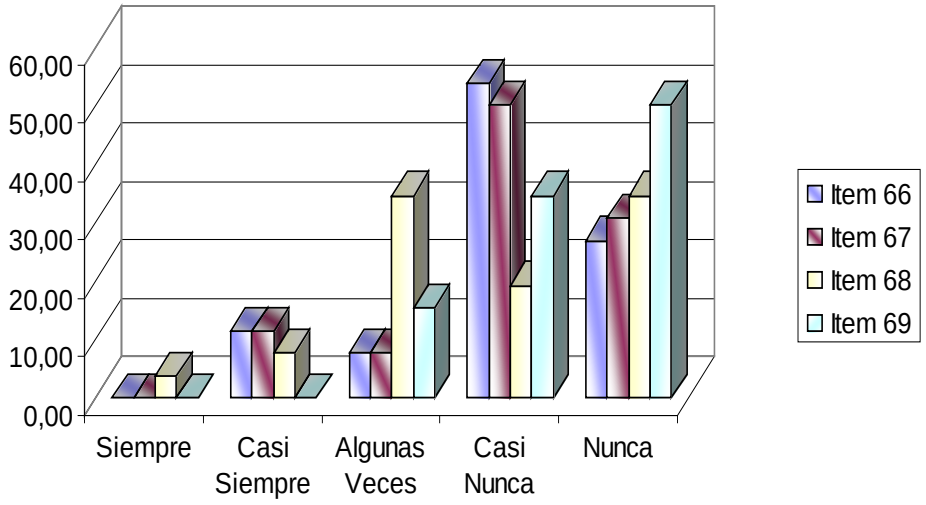



**Gráfico 11**. Porcentajes de las respuestas dadas a las preguntas sobre Cumplimiento.

El cuadro 14 y el grafico 11, reflejan las respuestas emitas por los sujetos de estudio. En el ítem 66 (¿Se definen, documentan y se actualizan todos los requisitos legales, reglamentarios y contractuales para cada sistema de información de la universidad?) y el ítem el 67 (¿Se implementa procedimientos apropiados para asegurarse del cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material protegido por derechos de propiedad intelectual, y sobre el uso de productos de software reservados?), las respuestas dadas son negativas, con un 73,08% y un 69,23% respectivamente para al alternativa Nunca.

Estas respuestas permite inferir que no se consideran o no se identifica la legislación aplicable a los sistemas de información que tiene la universidad, lo que hace suponer que no esta definido explícitamente y documentando todo lo que guarde relación con los requisitos legales, derecho de la propiedad intelectual, el uso de productos de software reservados.

En el ítem 68 (¿Se protegen los registros importantes contra pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales de la universidad?), el 6l, 54% opinó que Nunca y en el ítem 69 (¿Se planifican actividades de auditorias que involucren comprobaciones en los sistemas operativos y sistemas de información a fin de minimizar el riesgo de interrupción de los procesos de la universidad?), el 65,38% señaló que nunca. Estos resultados evidencian, la poca importancia que se le presta a la protección de la información clasificada.

*Observación directa*

En lo que respecta a la observación directa, no participante y sistemática de la realidad objeto de estudio y tomando como guía la norma ISO/IEC 27001:2005, en el anexo F, se encuentra los objetivos de control y controles listados en la Tabla A.1. En este sentido, la norma señala que " …. están directamente derivados y alineados con aquellos listados en los capítulos 5 al 15 de la Norma ISO/IEC 17799:2005. Las listas en la Tabla A.1 no son

exhaustivas y una organización puede considerar que son necesarios objetivos de control y controles adicionales" (p. 14). A continuación se detallan las observaciones realizadas en relación a cada uno de los objetivos de control.

**Cuadro 15**

**Observación directa**

| Cláusulas | Objetivo de control | Controles | Observación directa |
|---|---|---|---|
| A.5. Política de Seguridad | A.5.1. Política de Seguridad de la Información | A.5.1.1. Documento de la política de seguridad de la Información | No existe un documento de política de seguridad de información |
| A.6. Organización de la Seguridad de la información | A.6.1. Organización Interna | A.6.1.1. Compromiso de la dirección para la seguridad de la información | Existe un reglamento y los lineamientos de Tecnología aprobados por Consejo Universitario |
| | | A.6.1.3. Asignación de responsabilidades sobre la seguridad de la información | No están definidas claramente todas las responsabilidades de seguridad de la información |
| | A.6.2. Partes externas | A.6.2.1. Identificación de riesgos relacionaos a partes externas | No están identificados los riesgos a la información y recursos de procesamiento de la información |
| A.7. Gestión de activos | A.7.1. Responsabilidad por los activos | A.7.1.1. Inventario de activos | Se tiene una mediana documentación de lo que debería ser un inventario de servicios de información y de hardware |
| | | A.7.1.3. Utilización aceptable de los activos | No están implementadas las reglas para la utilización aceptable de la información y los activos asociados con las instalaciones. |
| | A.7.2. Clasificación de la información | A.7.2.1 Directrices de clasificación | No esta clasificada la información de acuerdo con su valor, sensibilidad y criticidad para la universidad. |
| | | A.7.2.2 Etiquetado y manejo de la información | No se han desarrollados procedimientos para etiquetar la información |

**Cuadro 15 (Continuación)**

| Cláusulas | Objetivo de control | Controles | Observación directa |
|---|---|---|---|
| A.8. Seguridad de recurso humanos | A.8.1. Antes del empleo | A.8.1.1 Roles y responsabilidades | No están documentadas las responsabilidades de seguridad de los empleados, contratistas y usuarios. |
| | | A.8.1.3. Términos y condiciones de empleo | Los empleados, contratistas y usuarios no firman acuerdos donde se establezcan responsabilidades por la seguridad de la información de la universidad. |
| | A.8.2. Durante el empleo | A.8.2.3 Proceso disciplinario | No existe proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad |
| | A.8.3. Terminación o cambio de empleo | A.8.3.1. Responsabilidades de la terminación | No están definidas claramente las responsabilidades para llevar a cabo la terminación o cambio de empleo |
| | | A.8.3.2 Devolución de los activos | No se cumple en su totalidad la devolución de todos los activos de la universidad una vez terminado la relación laboral. |
| | | A.8.3.3. Retiro de los derechos de acceso | Se mantienen lazos de amistad y se observa que empleados que han sido cambiados de oficinas mantienen acceso a la información y recursos para el procesamiento de la información |
| A.9 Seguridad física y ambiental | A.9.1 Áreas seguras | A.9.1.1 Perímetros de seguridad | El cuarto de cableado principal y de servidores no presenta ningún tipo de seguridad, la puerta principal es de formica y vidrio, las paredes son de formica y el techo está desprotegido, ver foto 1 y2. |

**Cuadro 15 (Continuación)**

<table>
<tr><td colspan="2">  </td><td colspan="2">  </td></tr>
<tr><td colspan="2">Foto 1: Puerta de la Sala de Cableado Principal y Servidores</td><td colspan="2">Foto 2: Pared y Techo de la Sala de Cableado principal y Sala de Servidores</td></tr>
<tr><td></td><td>A.9.2. Seguridad de los equipos</td><td>A.9.2.2. Seguridad del cableado</td><td>Se observa que el cableado de energía eléctrica y de comunicaciones que transporta datos no está protegido, se violentan todas las normas del cableado estructurado, no esta certificado.</td></tr>
<tr><td>  </td><td>  </td><td>  </td><td>  </td></tr>
<tr><td>  </td><td>  </td><td>  </td><td>  </td></tr>
</table>

**Cuadro 15 (Continuación)**

| Cláusulas | Objetivo de control | Controles | Observación directa |
|---|---|---|---|
| A.10 Gestión de comunicaciones y operaciones | A.10.1 Procedimientos y responsabilidades de operación | A.10.1.1. Documentación de procedimientos operativos | Los viejos sistemas de información no presentan ningún tipo de información, en cambio el SAI tiene toda la documentación técnica, pero el personal la desconoce, debe dársele adiestramiento. |
| | A.10.3 Planificación y aceptación del sistema. | A.10.3.1. Gestión de la capacidad | En relación al SAI no se realizaron los seguimientos de los requisitos del nuevo sistema, de allí que el sistema ha presentado tantas fallas y se ha dificultado tanto la puesta en producción. |
| | A.10.4. Protección contra código malicioso y movible | A.10.4.1. Controles contra código malicioso. | Existen antivirus en las estaciones de trabajo, pero los usuarios no tienen conciencia y bajan información no autorizada lo cual ponen en riesgo a los sistemas de información. |
| | A.10.5. Copia de Seguridad | A.10.5.1 Copia de seguridad de la información. | No se tienen respaldo o copias de seguridad de la información y software. |

**Cuadro 15 (Continuación)**

| Cláusulas | Objetivo de control | Controles | Observación directa |
|---|---|---|---|
| | A.10.6 Gestión de seguridad de la red. | A.10.6.1 Control de la red | La mayor debilidad que presenta el Vicerrectorado de Puerto Ordaz es no contar con un Administrador de Red y uno en Seguridad, lo cual afecta gravemente en la seguridad de los sistemas y aplicaciones que se encuentran en producción. |
| | A.10.7 Manejo de medios removibles. | A.10.7.2 Disposición de medios | No existen procedimientos formales para eliminar cualquier elemento que contiene información. |
| | | A.10.7.3 Procedimiento de manejo de la información | No existen procedimiento para el manejo y almacenamiento de la información. |
| | A.10.10 Seguimiento | A.10.10.1 Registro de auditoria | No se auditan las logs que registran actividad y eventos de seguridad. Tampoco se monitorea el uso de los sistemas. |
| | | A.10.10.5 Registro de fallas | No existen |
| | | A.10.10.6 Sincronización de relojes | No se sincronizan toda la plataforma de servidores |
| A.11 Control de accesos | A.11.1 Requisitos del negocio para el control de accesos. | A.11.1.1. Requisitos del negocio para el control de accesos. | No existe una política de control de acceso. |
| | A.11.2 Gestión de accesos de usuarios | A.11.2.1 Registro de usuarios | No existe un procedimiento formal. |
| | | A.11.2.3 Gestión de contraseñas de usuario | No se lleva una administración formal de asignación de contraseñas. |
| A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información | A.12.1 Requisitos de seguridad de los sistemas de información. | A.12.1.1 Análisis y especificación de los requisitos de seguridad | No se especifican los requisitos de control de seguridad en los sistemas de información |
| | A.12.2 Procesamiento correcto en las aplicaciones | A.12.2.1 Validación de datos de entrada | Existen procedimientos de validación de datos de entrada elementales, pero no garantizan que los datos sean correctos. |

**Cuadro 15 (Continuación)**

| Cláusulas | Objetivo de control | Controles | Observación directa |
|---|---|---|---|
| | | A.12.2.2 Control de procesamiento interno | No existen comprobaciones de validación en los sistemas |
| | | A.12.2.4 Validación de los datos de salida | La información procesada por los sistemas de información es revisada manualmente. |
| A.13 Gestión de los incidentes de seguridad de la información | A.13.1 Reportar los eventos y debilidades de seguridad de la información | A.13.1.1 Reporte de los eventos de seguridad de información | No existen registros de los incidentes de seguridad. |
| | | A.13.1.2 Reporte de debilidades de seguridad | No se observo ningún reporte de debilidades sospechadas a los sistemas. |
| A.14 Gestión de continuidad del negocio. | A.14.1 Aspectos de seguridad de la información de la gestión de continuidad del negocio | A.14.1.2 Continuidad del negocio y evaluación de riesgo | No están identificados los eventos de seguridad que causan interrupciones al servicio en la universidad. |
| | | A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información. | No existen planes de contingencias para mantener y recuperar las operaciones en el menor tiempo posible. |
| A.15 Cumplimiento | A.15.1 Cumplimiento de requisitos legales | A.15.1.1 Identificación de la legislación aplicable. | Los sistemas de información no tienen ningún tipo de documentación. |
| | | A.15.1.2 Derechos de propiedad intelectual (DPI) | El SAI si presenta documentación técnica y tiene licencia de ORACLE. |
| | | A.15.1.3 Protección de los registros de la organización. | Los archivos de información de cada una de las oficinas presentan poca protección. |
| | A.15.3 Consideraciones de auditoria de los sistemas de información | A.15.3.1 Controles de auditoria de los sistemas de información | No se planifican actividades de auditoria que involucren comprobaciones en los sistemas operativos. |

*Conclusiones del Diagnóstico*

Tomando en consideración los objetivos de la investigación y el análisis e interpretación de las respuestas dadas por los sujetos de estudio en el

instrumento aplicado y las observaciones hechas directamente por la investigadora, las conclusiones del estudio son las siguientes:

No existe un documento de política de seguridad de la información

En referencia a la organización de la seguridad de la información no se llevan eficazmente las políticas de seguridad de la información y no están definidas claramente todas las responsabilidades individuales para alcanzarla. Igualmente, no están definidos los requisitos para los acuerdos de confidencialidad de la información, ni se consideran todos los requisitos de seguridad antes de dar acceso al cliente o usuario de la información externo a la universidad.

No están establecidos los perímetros de seguridad para las áreas que contienen información crítica de la universidad.

No se cumplen los procedimientos para permitir el acceso sólo al personal autorizado.

Se tiene poco conocimiento para proteger los procesos administrativos críticos de la universidad de los efectos de fallas significativas de los sistemas de información y asegurar su reanudación oportuna.

No se lleva una correcta administración y control de la red, es decir, no se implementan todas las medidas posibles para evitar amenazas y mantener la seguridad de los sistemas y aplicaciones que circulan por ella.

No se realizan revisiones periódicas y procedimientos de monitorización del uso de los sistemas.

No existen políticas de control de acceso a la información universitaria.

No existen planes de continuidad del negocio.

*Recomendaciones*

Los resultados de la investigación fueron analizados utilizando la norma ISO/IEC 27001:2005, de allí se presentan las siguientes recomendaciones:

Se deben realizar dos documentos para considerar la seguridad de la información: el primero será un manual de política de seguridad de la información y el segundo documento será el plan de seguridad, como nivel de planeamiento o táctico.

El documento de política de seguridad de la información debe ser publicado y divulgado a toda la comunidad unexpista así como las partes externas pertinentes.

Dar a conocer el resultado de la investigación a las autoridades nacionales y regionales para que apoyen activamente la seguridad de la información dentro de la universidad, a través de un compromiso demostrado, con la asignación explícita de las responsabilidades de seguridad de la información.

Todo activo de la universidad debe estar inventariado con el máximo de detalles posible, igualmente debe ser clasificado por niveles de importancia.

Diseñar procedimientos para el control de accesos y seguridad perimetral en general.

Realizar el rediseño del cuarto principal de cableado y servidores que cumplan con los parámetros de diseño estándar, medidas de protección y alarmas contra incendios/humo, caídas de tensión, inundaciones, control de climatización (refrigeración y ventilación), sistemas vigilancia y control de accesos, limpieza, entre otros.

Diseñar e implementar procedimientos para la seguridad física en el almacenamiento y transporte de material informático y de comunicaciones: zonas y medidas de almacenamiento, metodología a seguir para el ingreso y egreso de este material, consideraciones particulares para el transporte del mismo (dentro y fuera de al organización), personal autorizado a recibir, entregar o sacar material, todas las medidas de control posibles.

En relación a la seguridad del recurso humano se recomienda que el Departamento de Personal y el grupo de seguridad y control de la ORTSI, redacten, conjuntamente, la documentación necesaria para la contratación de personal y la revocación de sus contratos (por solicitud, cambio o despido). En

la misma debe quedar bien claro las acciones a seguir para los diferentes perfiles de la universidad, basados en la responsabilidad del manejo de la información que tenga a su cargo.

Respecto a la organización de la seguridad de la información se recomienda registrar y mantener actualizada la cadena de contactos (internos y externos), con el mayor detalle posible (personas, responsabilidades, activos, necesidades, acuerdos, riesgos, entre otros) y los derechos y obligaciones de cualquiera de los involucrados. En este sentido, se debe diseñar e implementar una base de datos, que permita de forma amigable, la inclusión, eliminación y modificación de cualquiera de los campos. Una vez implementada la base de datos se deberá documentar la metodología de actualización, auditabilidad y periodicidad de informes de la misma.

Diseñar procedimientos para realizar copias de respaldo y recuperación de información.

Preparar al personal técnico y usuarios en cómo proceder ante los virus y realizar procedimientos de recuperación y verificación del buen funcionamiento de lo documentado.

Implementar controles técnicos, que evalúen permanentemente los servicios que la red ofrece. Para ello, se debe contar con un personal técnico altamente calificado en administración y seguridad de redes, así como también tener buenas herramientas tanto de hardware como de software para lograrlo.

### *Fase II. Factibilidad*

El estudio de factibilidad para determinar la viabilidad de un Sistema de Gestión de Seguridad de la Información para el sistema de información SAI, en el Vicerrectorado de Puerto Ordaz, tiene como objetivo verificar que la misma cumpla con ser una inversión atractiva a la Universidad. En este sentido se estudian tres tipos de factibilidad: operativa, técnica y económica.

*Factibilidad Operativa*

Para garantizar que se logre establecer el Sistema de Gestión de Seguridad de la Información para el Sistema Administrativo Integrado SAI, se procedió a tomar las siguientes medidas:

Publicación del reglamento de tecnología y servicio de información en la Web. El cual es soporte legal URL "http :// www .Unexpo.edu.ve/ documentos/ 05E0905.pdf".

Se realizó reunión con el Vicerrector de la UNEXPO – Puerto Ordaz y Director Administrativo para lograr un compromiso y el reconocimiento de las responsabilidades de seguridad de la información.

Se realizó reunión con el Director de la Oficina Central de Tecnología y Servicios de Información (OCTSI), el Coordinador Nacional de Tecnología y el líder técnico nacional del SAI, para lograr el compromiso necesario para el establecimiento del SGSI en la universidad.

Se llevaron a cabo reuniones con el personal de tecnología y los usuarios de los departamentos de Presupuesto, Contabilidad, Unidad de Compra, Unidad de Finanzas y Tesorería y almacén para ejecutar la fase de diagnóstico.

Se realizó un curso titulado "Implantación de un Sistema de Gestión de Seguridad de Información ISO 27001:2005" donde participó el personal técnico y administrativo involucrado con el sistema de información SAI, y en mesas de trabajo se realizó el análisis de riesgo de los activos de información.

Se impartió adiestramiento a los usuarios finales, respecto a normas básicas de seguridad de información y al nuevo reglamento de Tecnología.

Una vez realizado las actividades anteriores se puede afirmar que existe factibilidad operativa, los usuarios están en la mejor disposición y compromiso para el desarrollo del modelo planteado.

### *Factibilidad Técnica*

Se evaluó si se tienen las capacidades técnicas requeridas para cada alternativa del diseño que se esté considerando. De igual manera se consideró si la organización tiene el personal que posee la experiencia técnica requerida para establecer el Sistema de Gestión de Seguridad de la Información (SGSI) propuesto.

En este sentido como se evidenció en la fase de diagnóstico el Vicerrectorado de Puerto Ordaz, no posee suficiente personal adiestrado en el área de seguridad de la información, el sistema de información SAI presenta una serie de dificultades tales como: deficiencia de personal técnico calificado, falta de un plan de mejoramiento continuo para el personal involucrado a fin de elevar el nivel y la no existencia de normas y procedimientos administrativos. Adicionalmente, en lo referente a hardware, la infraestructura de red se encuentra fuera de norma.

Es de destacar que, la UNEXPO tiene varios proyectos relacionados para garantizar el desarrollo pleno del proyecto, entre ellos están: Red Corporativa de Datos del Vicerrectorado de Puerto Ordaz (en la fase de diseño), Normalización de la plataforma de las estaciones de trabajo, contratación de la prestación del servicio de telecomunicaciones entre las sedes principales de la UNEXPO, incluyendo transporte de voz, vídeo, dato y el servicio de Internet, contratación de personal técnico calificado, adquisición de equipos y el adiestramiento al personal usuario.

### *Factibilidad Económica*

Senn, J. (1987), señala que en el desarrollo de un sistema los beneficios financieros deben igualar o exceder los costo de inversión para la empresa, para poderse considerar factible económicamente.

En este sentido, el SAI es un sistema de información que permite realizar las operaciones administrativas de manera eficaz y eficiente, rendir cuentas en los lapsos previsto, minimizar los tiempos de respuestas a las peticiones realizadas por el ejecutivo nacional, tener información actualizada y consolidada del personal de la Unexpo y es una herramienta que permite el control y auditoría de las operaciones realizadas por el personal involucrado en los procesos administrativos. Como se ha evidenciado en todos los propósitos señalados anteriormente, la seguridad de la información juega un papel preponderante y cualquier monto de inversión para establecer un SGSI para el SAI, es considerado ínfimo respecto a los beneficios que se obtienen.

En conclusión, una vez analizado la factibilidad operativa, técnica y económica se corroboró que el establecimiento del Sistema de Seguridad de la Información para el Sistema Administrativo Integrado SAI, basado en las normas ISO/IEC 27001:2005 para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" Vicerrectorado de Puerto Ordaz es viable.

### *Fase III. Establecimiento del Sistema de Gestión de Seguridad de la Información S.G.S.I.*

Una vez identificada la necesidad en la fase de diagnóstico y estudiada la Factibilidad de establecer un Sistema de Gestión de Seguridad de la Información para un Sistema de Información tomando como caso de estudio el Sistema Administrativo Integrado SAI, en producción en la red de datos de la UNEXPO Vicerrectorado de Puerto Ordaz, se procedió al establecimiento del SGSI, cláusula 4.2 del ISO 27001:2005.

Establecimiento del S.G.S.I.

a. Definir el alcance y los límites del SGSI en términos de las características de la UNEXPO, localización, activos y tecnología.

b. Definir una política del SGSI en término de las características de la UNEXPO, su ubicación, activos y tecnología que:

c. Definir el enfoque de evaluación del riesgo de la organización.

1) Identificar una metodología de evaluación del riesgo que sea adecuada al SGSI, a la seguridad de la información y a los requisitos legales y reglamentarios.

2) Desarrollar criterios para la aceptación de los riesgos e identificar los niveles aceptables de riesgo.

d. Identificación los riesgos.

1) Identificar los activos dentro del alcance del SGSI y los dueños de esos activos.

2) Identificar las amenazas a esos activos.

3) Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.

4) Identificar los impactos que las pérdidas de confidencialidad, integridad y disponibilidad puedan tener sobre los activos.

e. Analizar y evaluar los riesgos

1) Evaluar los impactos que puedan resultar en fallas de seguridad, tomando en cuenta las consecuencias de una pérdida de la confidencialidad, integridad o disponibilidad de los activos.

2) Evaluar la probabilidad real de las fallas de seguridad que ocurren teniendo en cuenta las amenazas predominantes y vulnerabilidades, e impactos asociados con estos activos, y los controles implementados actualmente.

3) Estimar los niveles de riesgos

4) Determinar si los riesgos son aceptables o si requieren tratamiento utilizando los criterios para la aceptación de los riesgos establecidos en 4.2.1 c) 2).

f. Identificar y evaluar las opciones para el tratamiento de los riesgos.

g. Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos

h. Obtener la aprobación de los riesgos residuales propuestos por la dirección.

i. Obtener la autorización de la dirección para implementar y operar el SGSI.

j. Preparar una declaración de Aplicabilidad.

# CAPITULO IV

# PROPUESTA DEL ESTUDIO

## Justificación

Los sistemas de información y las tecnologías de información son de vital importancia como activos de la Universidad Nacional Experimental "Antonio José de Sucre", ya que, sin ellos la universidad presentaría serios problemas, entre los que se pueden mencionar: retrasos en la rendición de cuentas al Ejecutivo Nacional, retrasos en la generación de informes que permitan la toma de decisiones gerenciales, información no actualizada y no consolidada, lo cual incide negativamente en la realización de las operaciones administrativas, así como dificultad para controlar y auditar las operaciones realizadas por el personal involucrado en los procesos administrativos.

En este sentido, el sistema de información SAI, tiene como objetivo principal integrar los procedimientos manuales y automatizados para asegurar en la universidad un flujo de información adecuado que genere información actualizada, oportuna y que sirva de soporte en la toma de decisiones de cada uno de los niveles, con el fin de mejorar la gestión administrativa, financiera y no financiera, de la Institución.

Por todo lo ante planteado, el presente estudio plantea el establecimiento de un Sistema de Gestión para la Seguridad de la Información, basado en la norma ISO/IEC 27001:2005 para proteger la información administrativa de la universidad de una amplia gama de amenazas, tanto de orden fortuito como destrucción, incendio o inundaciones, como de orden deliberado, tal como fraude, espionaje, sabotaje, vandalismo, entre otros, con la finalidad de garantizar la confidencialidad, integridad y la disponibilidad de la información.

## Objetivos

### *Objetivo General*

Establecer un Sistema de Gestión para la Seguridad de la Información para el Sistema Administrativo Integrado SAI.

### *Objetivos Específicos*

Identificar los activos de información para el Sistema Administrativo Integrado SAI, en el Vicerrectorado de Puerto Ordaz.

Determinar las amenazas y las vulnerabilidades que podrían ser aprovechadas por las mismas.

Realizar el análisis y evaluación de los riesgos de seguridad de la información en el Sistema Administrativo Integrado SAI, en el Vicerrectorado de Puerto Ordaz, en el contexto de los riesgos globales de la universidad.

Preparar una declaración de la aplicabilidad que asegure la selección de controles de seguridad adecuados y proporcionales que protejan los activos de información del Sistema Administrativo Integrado SAI, en el Vicerrectorado de Puerto Ordaz, generando confianza a las partes interesadas.

## Descripción de la Propuesta

Para el diseño del Sistema de Gestión de Seguridad de la información para un Sistema de Información en producción en la red de datos de la Unexpo, Vicerrectorado de Puerto Ordaz, se utilizó la norma ISO/IEC 27001:2005, el cual adopta el enfoque de procesos basado en el ciclo Deming “Planificar – Hacer – Verificar – Actuar” (PHVA). Este modelo está basado en un enfoque racional para su desempeño y su perfeccionamiento en el tiempo. En primera instancia, el modelo exige que se siga una serie de prerrequisitos para que se establezca, a través de la fase denominada “Planificar”. Una vez establecido el modelo se implementa y opera,

siguiendo los lineamientos de la fase "Hacer". Luego que el modelo se ha implantado y está funcionando, se debe "monitorear y revisar" durante la fase "verificar" y por último, con base en lo observado, se procede a "Actuar" y tomar correctivos necesarios. En cada una de las cuatros fases del ciclo Deming, se colocan las cláusulas correspondientes. A continuación, se presentan la primera fase del modelo ISO 27001:2005.

**Establecimiento de un Sistema de Gestión de Seguridad de la Información**

El establecimiento de un sistema de gestión de seguridad de información tiene como objetivos entender cómo se debe proceder metodológicamente para efectuar una identificación de activos de información dado un alcance determinado, distinguir entre el análisis y evaluación del riesgo y visualizar la relación causa – efecto entre los elementos del riesgo.

A continuación se presenta el alcance del SGSI para el Sistema Administrativo Integrado, SAI.

*Alcance de un SGSI*

El Sistema de Gestión de Seguridad de la Información se realizó a un sistema de información, específicamente al Sistema Administrativo Integrado SAI, solamente para los módulos operativos actualmente, que son: Compras y Almacén, Contabilidad, Presupuesto y Tesorería. Estos módulos están instalados en las oficinas de Compra, Finanzas y Tesorería, Contabilidad, Presupuesto y ORTSI, ubicadas en el Edificio Administrativo y el Almacén General ubicado en la planta baja del Edificio de los Departamentos de Mecánica e Industrial, del Vicerrectorado de Puerto Ordaz. (Ver Anexo G y H).

Para poder identificar con precisión las interfaces y dependencias del SGSI con otras partes de la universidad y entidades externa, se optó por utilizar la metodología propuesta por Alexander (2007), el método de las elipses, definida como "… método

que permite, dado un determinado alcance de un SGSI, identificar sus interfaces, interdependencias con áreas y procesos, así como averiguar el tipo de memorando de entendimiento que existe o debiera de elaborarse, así como los contratos existentes y los grados de acuerdo necesarios" (p. 42).

En este sentido, se realizaron los siguientes pasos: a) Se determinó en la elipse concéntrica los distintos procesos y subprocesos que se realizan en los módulos de Compras y Almacén, Contabilidad, Presupuesto y Tesorería del sistema administrativo integrado, 2) Se identificó en la elipse intermedia las distintas interacciones que los procesos de la elipse concéntrica tiene con otros procesos de la universidad, c) Se identificaron aquellas organizaciones extrínsecas a la universidad que tienen cierto tipo de interacción con los procesos y subprocesos identificados en la elipse concéntrica y d) Se unió con flechas los tipos de interacción y la direccionalidad que tiene el flujo de información, la figura 4 muestra este método aplicado al sistema administrativo integrado (SAI).

Adicionalmente, la figura 5 permite entender la interconexión física de todos los equipos que permiten la comunicación del sistema administrativo integrado (SAI), los cuales son activos del SGSI.

### *Política de un SGSI*

Una vez determinado el alcance del SGSI, la UNEXPO debe establecer una clara política de seguridad para apoyar la implementación de la seguridad de información en la universidad. En este sentido, la ISO 17799:2005 plantea que el objetivo de la política es: "… proveer a la gerencia dirección y apoyo para la seguridad de la información".

Es importante señalar, que las políticas deben ser aprobadas por el Consejo Universitario y se deben dar a conocer a toda la comunidad unexpista. En el anexo H, se observan las políticas de seguridad de la información para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre".

**Figura 5.** Metodología de las elipses en el Sistema Administrativo Integrado (SAI). Autora 2007.

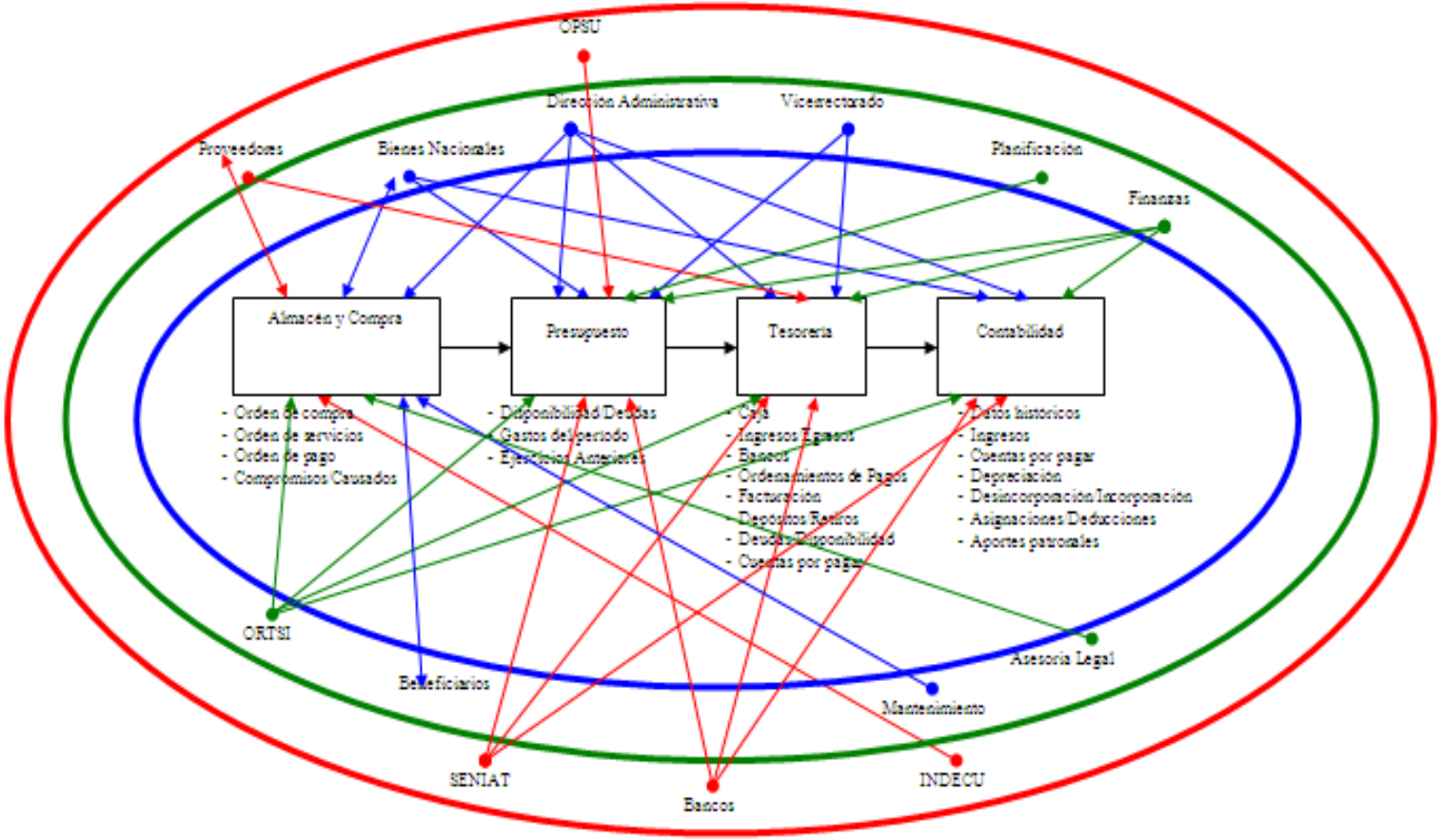
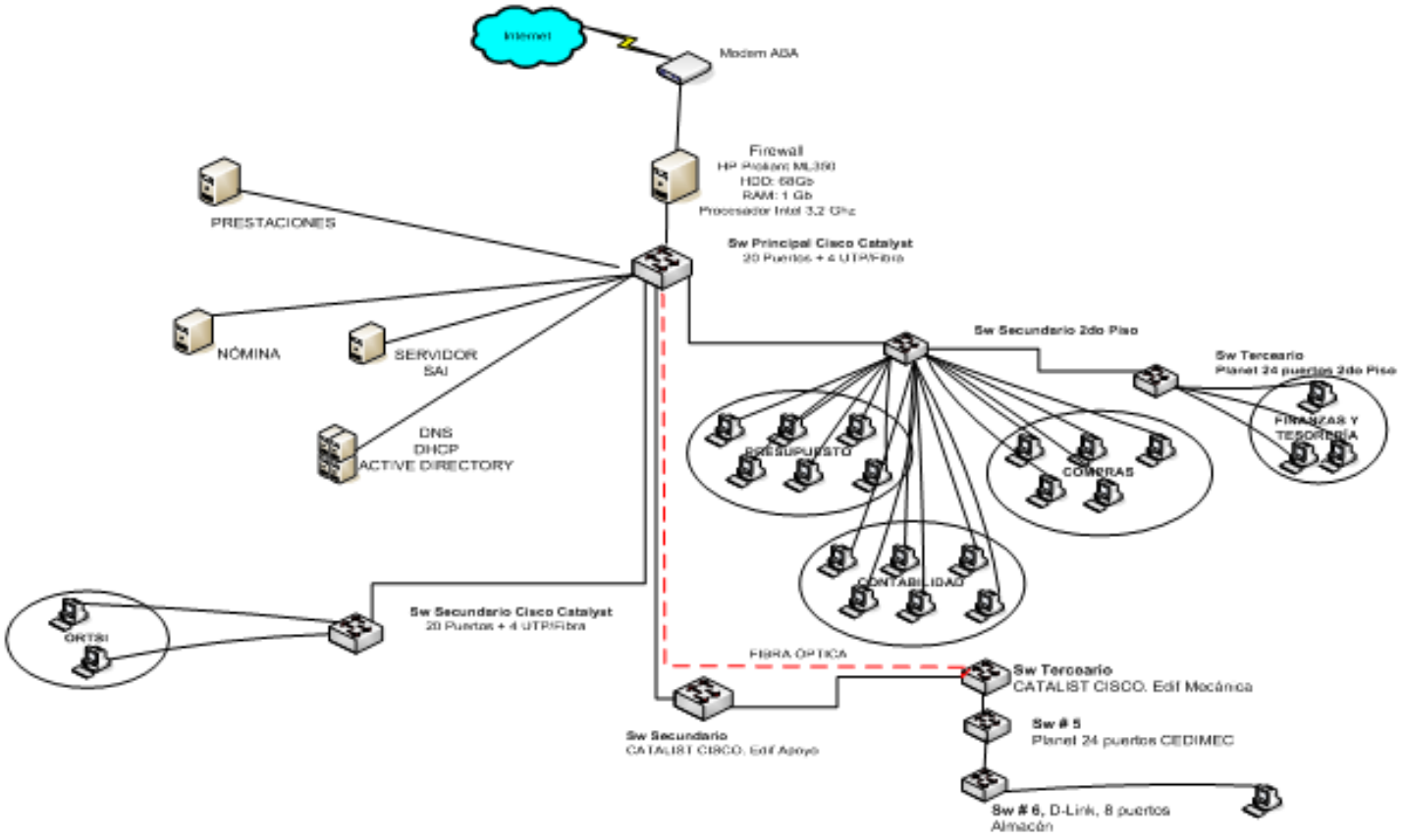


**Figura 6.** Plano lógico del Sistema Administrativo Integrado, SAI. Autora 2007.



*Enfoque de Evaluación riesgo*

El enfoque y la filosofía para el riesgo en una organización están determinados de manera muy precisa por el ISO/IEC 27001:2005. En este sentido, la metodología de evaluación de riesgo empleada fue la recomendada por Ormella, (2007), la herramienta CRAMM, la cual presenta la desventaja de que es una herramienta propietaria y el IT Baseline Protection Model del BSI Alemán, herramienta de libre acceso.

Las razones son: la herramienta CRAMM puede usarse con ISO 27001 así como para el manejo de riesgo de negocios. Esta herramienta utiliza una escala de 1 a 10 para la valorización de los activos, de 1 a 5 niveles para las amenazas y de 1 a 3 para las vulnerabilidades y el cálculo del riesgo de 1 a 7 según una matriz, mientras la BSI, permite establecer los riesgos en base a los activos, amenazas y contramedidas. Presenta una tabla de 200 amenazas clasificadas en cinco tipos: fuerza mayor, deficiencias organizacionales, fallas humanas, fallas técnicas y actos deliberados, tiene la desventaja de no trabajar directamente con vulnerabilidades. Es por ello que no es recomendable trabajar con una sola metodología, es importante conocer las bondades de cada una y aprovecharlas para adaptarla al sistema de gestión en estudio.

*Identificación del riesgo*

El cálculo de los riesgos de seguridad de información incluye normalmente el análisis y la evaluación del riesgo. El análisis del riesgo contempla: 1) Identificar los activos dentro del alcance del SGSI y los dueños de esos activos, 2) Identificar las amenazas a esos activos, 3) Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas y 4) identificar los impactos que las pérdidas de confidencialidad, integridad y disponibilidad puedan tener sobre los activos.

A continuación se presenta la tasación de los activos de información con respecto a los módulos del sistema de información SAI, de acuerdo a los criterios de confidencialidad, integridad y disponibilidad.

## Cuadro 16

Activos Primarios clasificados

**ACTIVOS PRIMARIOS CLASIFICADOS**

**Clase 1 - Componentes de Protección Genérica**
**Clase 2 - Infraestructura**
**Clase 3 - Sistemas clientes y Computadoras aisladas**
**Clase 4 - Servidores y redes**
**Clase 5 - Sistemas de Transmisión de Datos**
**Clase 6 - Telecomunicaciones**
**Clase 7 - Otros componentes IT**

**CLASE 1 - COMPONENTES DE PROTECCION GENERICA**

| Nro. | Nombre Activo Primario | Nivel | Descripción general |
|---|---|---|---|
| 1.1 | Organización | 8 | Conjunto de medidas generales y genéricas en el campo organizacional para una protección mínima en el sistema SAI y en IT tales como administración de medios de datos, procedimientos en el uso de contraseñas, entre otros. |
| 1.2 | Personal | 5 | Totalidad de cuestiones relacionadas con el personal en su influencia en el Sistema Administrativo Integrado SAI, desde su contratación, ausencias, entrenamiento, retiro, cambio de oficina, despido o jubilación. |
| 1.3 | Políticas de back up | 9 | Sistema de procedimientos sistemáticos y prevención de fallas técnicas, borrado o manipulación inadecuada para evitar que los datos se vuelvan inservibles o se pierdan. |
| 1.4 | Protección de virus | 9 | Prevención o detección de virus tan pronto como sea posible y minimización de posibles daños. |
| 1.5 | Información | 9 | Información clasificada |
| 1.6 | Gestión de hardware y software | 7 | Procedimientos de seguridad referidos al ciclo de vida de componentes de hardware y software. |

**CLASE 2 - INFRAESTRUCTURA**

| Nro. | Nombre Activo Primario | Nivel | Descripción general |
|---|---|---|---|
| 2.1 | Edificios | 2 | Construcción donde se realizan operaciones de procesamiento de datos del SAI. |
| 2.2 | Cableado | 5 | Diseño y disposición de líneas de comunicaciones y servicios adicionales. |
| 2.31 | Oficinas | 2 | Lugar donde se usan el sistema administrativo integrado, SAI. |
| 2.32 | Sala de Servidores | 9 | Lugar donde se instala el servidor SAI y componentes complementarios incluyendo los servicios de funcionamiento y prevención general. |
| 2.33 | Archivos de medios de datos | 6 | Lugar específico dentro de un ambiente donde se guardan medios de datos, típicamente de back up. |
| 2.34 | Cuarto de Cableado Secundario | 2 | Centros de conectividad, y las facilidades para su funcionamiento. |
| 2.4 | Gabinetes de protección | 3 | Armario para guardar medios de datos o hardware. |

**CLASE 3 - SISTEMAS CLIENTES Y COMPUTADORAS AISLADAS**

| Nro. | Nombre Activo Primario | Nivel | Descripción general |
|---|---|---|---|
| 3.1 | Laptops | 4 | Computadoras portátiles en general. |
| 3.2 | PCs bajo Win XP | 3 | PCs conectadas en red como clientes de un servidor. |

**Cuadro 16 (Continuación)**

| ACTIVOS PRIMARIOS CLASIFICADOS | | | |
|---|---|---|---|
| **CLASE 4 - SERVIDORES Y REDES** | | | |
| **Nro.** | **Nombre Activo Primario** | **Nivel** | **Descripción general** |
| 4.1 | Red soportada por servidor | 8 | Computador que provee servicios a una red independientemente del sistema operativo que corra. |
| 4.2 | Servidor Linux | 8 a 10 | Computador bajo sistema operativo Unix/Linux que provee servicios en una red. |
| 4.3 | Servidor Windows | 8 a 10 | Computador bajo sistema operativo Windows que provee servicios en una red. |
| 4.4 | Componentes activos de red | 9 | Routers, switches y demás dispositivos activos de conectividad; topología, configuración, selección y protocolos de comunicaciones. |
| 4.5 | Gestión de redes y sistemas | 6 | Operaciones centralizadas de chequeo y monitoreo centralizado de una red, y administración de usuarios, distribución de software y manejo de aplicaciones. |
| **CLASE 5 - SISTEMAS DE TRANSMISION DE DATOS** | | | |
| **Nro.** | **Nombre Activo Primario** | **Nivel** | **Descripción general** |
| 5.1 | Intercambio de medios de datos | 4 | Manejo de medios de datos en tránsito no electrónico; almacenamiento físico en origen y destino. |
| 5.2 | Modem | 5 | Dispositivo de comunicación por línea discada o banda ancha |
| 5.3 | Firewall | 10 | Dispositivo de protección entre dos redes, típicamente en el acceso a Internet. |
| **CLASE 6 - TELECOMUNICACIONES** | | | |
| **Nro.** | **Nombre Activo Primario** | **Nivel** | **Descripción general** |
| 6.1 | Máquina de fax | 2 | Dispositivo de envío manual de imágenes de documentos vía telefónica. |
| **CLASE 7 - OTROS COMPONENTES IT** | | | |
| **Nro.** | **Nombre Activo Primario** | **Nivel** | **Descripción general** |
| 7.1 | Software y aplicaciones | 7 | Manejo de los aspectos de seguridad del ciclo de vida del Sistema Administrativo Integrado SAI: requerimientos, selección, pruebas, aprobación, instalación, desinstalación. |
| 7.2 | Bases de datos | 10 | Selección, instalación, configuración y operación de un sistema de bases de datos por medio de un DBMS. |

Una vez determinado los activos de acuerdo con el alcance del Sistema de Gestión de Seguridad de la Información, se procede a identificar las amenazas y vulnerabilidades del mismo.

*Identificación de amenazas y vulnerabilidades*

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus activos. Al respecto, Alberts y Dorofee (2003), define la amenaza como la indicación de un potencial evento no deseado. En esta

definición, los autores se refieren a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural.

Para una empresa, las amenazas pueden ser de distintos tipos con base en su origen. En el cuadro 17 se muestran una clasificación de las distintas clases de amenazas que pueden estar afectando los activos de una empresa.

**Cuadro 17**

**Amenazas definidas**

**AMENAZAS DEFINIDAS**

| Tipo | Niveles de Amenazas |
|---|---|
| 1 Fuerza Mayor | Muy Baja 1 |
| 2 Deficiencias organizacionales | Baja 2 |
| 3 Fallas humanas | Media 3 |
| 4 Fallas técnicas | Alta 4 |
| 5 Actos deliberados | Muy alta 5 |

**TIPO 1 - FUERZA MAYOR**

| Nro. | Nivel | Descripción | Detalle |
|---|---|---|---|
| 1.1 | 3 | Pérdida de personal | Por enfermedad, accidentes, muerte, huelgas que conduzcan a que tareas IT cruciales no se puedan efectuar. |
| 1.2 | 4 | Fallas de los sistemas IT | De un único componente que puede afectar toda la operación IT. Fallas del ISP. |
| 1.3 | 2 | Rayos | Que causen alto voltaje o el disparo de extinguidores automáticos de incendio paralizando las operaciones. |
| 1.4 | 4 | Incendio | Además del daño directo el causado por el agua con que se ataca el incendio. Descuido en el manejo de material combustible, uso impropio de dispositivos eléctricos, fallas en el equipamiento eléctrico. |
| 1.5 | 3 | Inundación | Por lluvia, anegamientos, agua usada en un incendio, bloqueo de drenajes. |
| 1.6 | 2 | Cables quemados | Corte de conexiones, formación de gases agresivos, material aislante no resistente al fuego, fuego humeante sin llama en cables empaquetados. |
| 1.7 | 2 | Polvo y suciedad | Por trabajos realizados en paredes, pisos, actualizaciones de hardware, materiales de empaquetado. |
| 1.8 | 2 | Efectos de catástrofes en el ambiente | En los alrededores del campus UNEXPO. Desde accidentes técnicos y daños por colisiones hasta huelgas. |
| 1.9 | 2 | Problemas causados por grandes eventos públicos | Interrupción de operaciones, violencias, cortes de líneas de transmisión. |
| 1.10 | 2 | Tormentas | Desprendimiento de instalaciones en azoteas (por ejemplo aire acondicionado), paredes débiles que caen y cortan cables. |

**Cuadro 17 (Continuación)**

| TIPO 2 - DEFICIENCIAS ORGANIZACIONALES | | | |
|---|---|---|---|
| 2.1 | 4 | Falta o insuficiencia de reglas de seguridad en general | Organización: asignación responsabilidades, gestión de recursos |
| 2.2 | 5 | Conocimiento insuficiente de documentos sobre reglas y procedimientos | Falta información procedimientos manejo disquetes y e-mails. |
| 2.3 | 2 | Recursos incompatibles o inadecuados | Memoria principal o espacio en disco insuficiente. |
| 2.4 | 3 | Monitoreo insuficiente de las medidas de seguridad IT | No se imprimen las entradas de consola para su análisis. Los servidores que se usan para comunicaciones externas deben chequearse semanalmente en cuanto a integridad. |
| 2.5 | 2 | Mantenimiento faltante o inadecuado | Baterías de UPS. Presión extinguidores. |
| 2.6 | 1 | Uso no autorizado de derechos | Derechos de admisión a hard o soft asignados a personas equivocadas, o un derecho abusado. |
| 2.7 | 1 | Uso no controlado de recursos | Los medios privados que pueden entrar virus en las PCs. Productos de limpieza no adecuados. |
| 2.8 | 2 | Ajuste deficiente a los cambios en el uso de IT | Cambios de derechos en personal por vacaciones. No se imprimen los cambios de procedimientos. |
| 2.9 | 3 | Medio de datos no disponible cuando se lo requiere | Falta de rotulación adecuada o almacenamiento en lugares no previstos. |
| 2.10 | 3 | Dimensionamiento insuficiente de redes y centro de cómputo | Sala de servidores, centros de cómputo. Capacidad red y computadores, extendida en línea por volumen de datos o nuevos servicios. Cableado. Nuevas normas. |
| 2.11 | 2 | Documentación insuficiente del cableado | Consecuencias por desconocimiento cableado interno y externo. Trabajos de terceros. |
| 2.12 | 1 | Protección inadecuada de dispositivos de distribución de energía | Si son accesibles en corredores y cajas de escaleras, cualquier persona podría manipularlos y causar una caída de energía. |
| 2.13 | 2 | Cambios no regulados de usuarios en laptops | Ante cambios de usuarios en móviles puede quedar información sensible o virus. Y si no se controlan esos cambios no se sabe quién los usó y cuándo. |
| 2.14 | 1 | Etiquetado inadecuado de medios de datos | El que recibe podría no poder identificar el origen, la información almacenada, o el propósito. Podría afectar una secuencia, los errores y correcciones que no quedan claros. |
| 2.15 | 1 | Entrega impropia de medios de datos | Puede caer en manos impropias. Direccionamiento, empaquetado, fallas de responsabilidad en recepción. |
| 2.16 | 1 | Provisión inadecuada de papel para máquinas de fax | Papel, batería |
| 2.17 | 4 | Pérdida de confidencialidad de datos sensibles de la red a proteger | Si no hay protección con un firewall queda mucha información expuesta a Internet y hasta el resto puede deducirse u obtenerse con mayor facilidad. |

**Cuadro 17 (Continuación)**

| | | | |
|---|---|---|---|
| 2.18 | 2 | Reducción de la velocidad de transmisión o ejecución debido a funciones P2P | Funciones P2P en un mismo servidor Windows; restricción de ancho de banda, retardos. |
| 2.19 | 3 | Procedimientos faltantes o inadecuados para test y liberación de software | Si no se hacen pruebas antes de instalar algo nuevo, pueden volverse amenazas. Sobre todo si se lo hace sin mayores conocimientos. |
| 2.20 | 3 | Documentación faltante o inadecuada | Varios: descripción de productos, uso por administrador y usuario, y de sistema. Impactan la selección y toma de decisiones. Archivos temporales con información sensible, configuraciones que cambian y pueden afectar aplicaciones que estaban corriendo, cableado. |
| 2.21 | 2 | Violación de derechos de autor | Software pirata. |
| 2.22 | 4 | Prueba de software con datos de producción | Pensando que así se obtiene una valuación definitiva de las funciones y performance. Puede ser que sean copias y en un ambiente aislado pero como son datos reales están expuestos a terceros no autorizados a leer esa información. Y si se hacen directamente en operación, a la pérdida de confidencialidad se agregan la de integridad y disponibilidad. |
| 2.23 | 2 | Planificación inadecuada de los dominios | En redes Win NT pueden ocurrir relaciones de interconfianza inadecuadas. Esto puede darse especialmente cuando los derechos de acceso se hacen muy amplios asumiendo que nadie de otro dominio accederá los recursos locales. |
| 2.24 | 3 | Protección inadecuada del sistema Windows | Por default hay amplios derechos de acceso al sistema de archivos y registro. |
| 2.25 | 1 | Restricción inapropiada del ambiente de usuarios | Algunas permitidos, prohibidos todas los demás. O la inversa: algunas prohibidas, permitidas todas las demás. |
| 2.26 | 2 | Mecanismos de seguridad de bases de datos faltantes o implementados inadecuadamente | El software de BD trae generalmente mecanismos de seguridad que protegen los datos de accesos no autorizados, pero estos mecanismos generalmente no son automáticos sino que se activan manualmente por parte del administrador. Sino no se podría garantizar confidencialidad e integridad, así como tampoco identificar violaciones de seguridad de registro. Podría haber pérdidas de datos y la destrucción de la BD. |
| 2.27 | 2 | Complejidad del DBMS | Si los mecanismos de seguridad propios no son suficientes, o si las medidas que recomienda el fabricante no se tienen en cuenta. En cuanto al concepto de DB: que los datos específicos de la aplicación no se almacenen en medios separados, o el no uso de db triggers y procedimientos almacenados, o si su uso no es consistente resulta proclive a manipulaciones que pueden afectar la integridad. |
| 2.28 | 3 | Complejidad del acceso a las bases de datos | Que los derechos sean muy restrictivos y no se puedan realizar algunas tareas. O que sean muy laxos permitiendo manipulaciones. Si los usuarios pueden acceder directamente a la DB. Salvaguardas insuficientes para el acceso remoto a la DB. Restricciones a las consultas. |
| 2.29 | 1 | Organización deficiente del cambio de usuario en bases de datos | Varios usuarios compartiendo una DB en la misma estación de trabajo y que no se deslogean. |

**Cuadro 17 (Continuación)**

| | | | |
|---|---|---|---|
| 2.30 | 3 | Deficiencias conceptuales de las redes | Usuarios trabajando en grupos teniendo presente confidencialidad e integridad. Nuevas aplicaciones con mayores exigencias de ancho de banda. Pérdida de disponibilidad con redes propietarias. Componentes que no soportan ciertos protocolos. |
| 2.31 | 1 | Descripción inadecuada de archivos | Varios mensajes del mismo origen sin identificación adecuada, cuando a una serie de mensajes se hacen correcciones en uno de ellos. |
| 2.32 | 2 | Almacenamiento inadecuado de un medio en casos de emergencias | Por falta de capacidad de almacenamiento que se haga back up solamente de los archivos log y de configuración. |
| 2.33 | 1 | Operación de componentes no registrados | Componentes agregados desconocidos para el administrador. Una PC en la que se deja el "public" en el SNMP. |
| 2.34 | 4 | Manejo inapropiado de los incidentes de seguridad | Las posibilidades siempre existen y los incidentes no pueden eliminarse. Lo importante es la respuesta dada a un incidente. Casos como nuevos virus, control del material que se mantiene en un servidor Web que puede indicar un signo de ataque, nuevas vulnerabilidades que se descubren en los sistemas IT, datos corporativos que han sido manipulados. Si no hay procedimientos apropiados para manejar incidentes se puede llegar a tomar decisiones incorrectas que afecten la seguridad (componentes que se mantienen pese a conocerse serias debilidades, o viceversa, se saca algo cuyo riesgo es menor. |
| 2.35 | 3 | Administración inapropiada de derechos de acceso | Porque intervienen muchas personas. No hay registro sistemático de todos los usuarios; quedan cuentas abiertas, o se acumulan derechos por cambios de actividades. Cuidado especial con los grupos. |
| | | **TIPO 3 - FALLAS HUMANAS** | |
| 3.1 | 2 | Pérdida de confidencialidad /integridad de datos por errores de los usuarios | Impresiones en papel que caen en manos inapropiadas. Disquetes despachados sin borrar los datos anteriores. Derechos de acceso incorrectos que pueden hacer que se modifiquen datos críticos. |
| 3.2 | 2 | Destrucción negligente de equipamiento o datos | Apagado computador al aparecer mensaje de error que puede producir errores de integridad. Humedad de café, etc. |
| 3.3 | 4 | No cumplimiento con las medidas de seguridad IT | Por negligencia o pruebas insuficientes. Podrían producirse daños que podrían haberse previsto o al menos minimizados. Depende de la persona actuante. |
| 3.4 | 1 | Conexión inadmisible de cables | Por documentación o etiquetado deficiente. Puede ocasionar el paso de datos adicionales o a direcciones equivocadas. |
| 3.5 | 2 | Daño inadvertido de cables | Por falta protección, cables colgando, en el suelo, perforaciones, agua. |
| 3.6 | 2 | Riesgos planteados por el personal de limpieza o externo | Manejo inapropiado de equipos, o uso indebido o hurto de componentes. |
| 3.7 | 2 | Uso impropio del sistema IT | Negligencia o ignorancia de medidas de seguridad. Falta de información de la operación y funcionamiento correcto del sistema IT. |

**Cuadro 17 (Continuación)**

| | | | |
|---|---|---|---|
| 3.8 | 3 | Administración inapropiada de los sistemas IT | Negligencia o ignorancia de medidas de seguridad. Si algunos puntos de acceso se crean o no se deshabilitan por no ser necesarios para la operación regular o proclive a errores. |
| 3.9 | 1 | Transferencia de registros de datos incorrecta o indeseada | Datos anteriores que no debieran aparecer. Si se envían electrónicamente las listas podrían no estar actualizadas respecto de personal que no trabaja más. |
| 3.10 | 3 | Exportación incorrecta de sistemas de archivos bajo Linux | Los discos exportados en Linux pueden montarse por cualquier computador con el nombre definido en /etc/exports. El usuario de ese computador puede asumir cualquier UID/GID, es decir que sólo se pueden proteger los archivos pertenecientes al root. Los archivos de todos los demás usuarios están completamente desprotegidos, especialmente los que pertenecen a usuarios privilegiados como bin o daemon. |
| 3.11 | 4 | Configuración impropia del sendmail | Errores de configuración que permitan obtener las IDs de usuario y grupo que estén setados con las opciones u y g (normalmente daemon). |
| 3.12 | 1 | Administración incorrecta del sitio y derechos de acceso a los datos | Derechos de acceso incorrectos pueden permitir acceder a datos de auditoria así como ocultar las manipulaciones. |
| 3.13 | 1 | Cambio incorrecto de usuarios de PC | Desregistro de un usuario antes de logearse otro por negligencia o conveniencia. Fallaría la auditoria de logs. |
| 3.14 | 2 | Administración impropia de una DBMS | Administración negligente o impropia de la DB, así como derechos de acceso demasiado generoso, irregularidad o falta de monitoreo, backups inadecuados, UDs inválidas pero no desactivadas, pueden producir pérdida de datos, manipulación intencional o inadvertida de datos, acceso no autorizado a datos confidenciales, pérdida de integridad de la DB, caída y destrucción. |
| 3.15 | 3 | Configuración inadecuada de los componentes activos de las redes | Configuración incorrecta de VLAN, tablas de enrutado en subredes sea el enrutado estático o de actualización automática por medio del RIP u OSPF, componentes que filtran protocolos y direcciones de red pero que también pueden permitir las conexiones de sistemas IT externos dentro de la red protegida. |
| 3.16 | 1 | Deshabilitación de un servidor en operación | Servidor de gestión deshabilitado se pierde lo que estaba en memoria, aparecerán inconsistencias en los datos administrados. |
| 3.17 | 3 | Errores en la configuración y operación | Información que ofrece el servidor Web, o un servidor DNS, contenidos ejecutables de un e-mail, archivos bajados, programas que se abren sin ser necesarios y que pueden usarse para ataques. |
| 3.18 | 4 | Manejo inapropiado de contraseñas | Que no las conozcan otras personas. Token cards perdidas. Nombres comunes, etc. |
| 3.19 | 3 | Falta de cuidado en el manejo de la información | Contraseñas escritas a la vista, información divulgada en celulares, viajando. Reparación de una máquina por cambio y quedan los datos para otro usuario. |

## Cuadro 17 (Continuación)

| TIPO 4 - FALLAS TECNICAS | | | |
|---|---|---|---|
| 4.1 | 2 | Disrupciones en la fuente de energía | Cortes breves (UPS), UPS en condiciones para switch back. |
| 4.2 | 2 | Fallas de las redes internas de alimentación | Electricidad, teléfono, aire acondicionado. También por temperatura, agua, etc. |
| 4.3 | 2 | Medios de datos defectuosos | Discos con caída de la cabeza, cintas y cassettes por impactos mecánicos directos. CD por ralladuras superficiales. |
| 4.4 | 5 | Reconocimiento de vulnerabilidades en el software | Errores no intencionales del programa no conocidos por usuario. Se siguen encontrado debilidades. Contramedida |
| 4.5 | 4 | Diversidad de posibilidades de acceso a sistemas IT en red | Además del ingreso "directo" con contraseña, por sendmail que puede introducir textos, ftp anónimo sin contraseña, telnet registro completo. Win más seguro. |
| 4.6 | 1 | Errores de transmisión de fax | Los errores en la ruta de transmisión o en los dispositivos de conexión pueden producir pérdidas o que la información se vuelva ilegible. |
| 4.7 | 1 | Defectos técnicos de las máquinas de fax | Disponibilidad e integridad pueden verse afectadas. |
| 4.8 | 1 | Pérdida de datos debido al agotamiento del medio de almacenamiento | No se puede almacenar más datos, email entrante se rechaza, no se pueden mantener auditoria. |
| 4.9 | 4 | Fallas de una base de datos | Por errores, o acto de sabotaje puede tener amplias consecuencias dependiendo de las funciones y significado de la DB. Consecuencias pérdidas financieras, interrupción parcial o total de las operaciones. |
| 4.10 | 2 | Pérdida de datos en una base de datos | Por manipulación inadvertida, caídas de la DB e intrusiones deliberadas. Podría impedirse la ejecución, perderse la correlación de datos. Puede ocurrir cuando se cambia el modelo de la DB. |
| 4.11 | 3 | Pérdida de integridad/consistencia de una base de datos | Corrupción parcial o datos no inteligibles por manipulación de datos no intencionales, chequeos inadecuados de la sincronización de transacciones, e intrusiones deliberadas. |
| 4.12 | 5 | Falla o mal funcionamiento de un componente de red | Puede afectar a toda la red o secciones de la misma. Podría ser un switch que afecta toda su área, o componentes activos en el camino de las comunicaciones (y no hay caminos redundantes), o para redundancia o balanceo de carga (con las consiguientes restricciones de ancho de banda). |
| 4.13 | 4 | Autenticación faltante o de pobre calidad | Pueden hacer que personas no autorizadas logren acceder al sistema, que no se puedan identificar las causas de problemas, o no se pueda determinar el origen de los datos. Esto ocurre por contraseñas débiles, o no se los cambia con regularidad, o hay fallas de seguridad frente a los que no se reacciona. |
| 4.14 | 2 | Falla de componentes de un sistema de gestión de red o de sistemas | Pueden fallar los componentes administrados, o los de monitoreo mismo, la estación central de gestión, o algún elementos de conmutación durante la transmisión correspondiente. |
| 4.15 | 4 | Vulnerabilidades o errores de software | Tanto standard como los demás. Quizás encripción de standard no es suficiente. Funciones sin documentar. Errores de seguridad en la programación, desborde de buffers. |

**Cuadro 17 (Continuación)**

| | | | |
|---|---|---|---|
| 4.16 | 1 | Reconocimiento automático del CD-ROM | Si el reconocimiento de CD-ROM está activado en Windows 95 puede ejecutarse algún programa peligroso en el momento del arranque. |
| | | **TIPO 5 -ACTOS DELIBERADOS** | |
| 5.1 | 2 | Manipulación/destrucción de equipamiento o accesorios de IT | Equipos, accesorios y documentación. Inspección indebida de datos sensibles. Destrucción de medios de datos. |
| 5.2 | 3 | Manipulación de datos o software | Adquisición errónea de datos, cambios derechos de acceso, modificación de datos contables o de mail. Depende de los derechos de acceso de la persona en cuestión. |
| 5.3 | 3 | Ingreso no autorizado a un edificio | Robo o alteración al poder entrar especialmente de noche. |
| 5.4 | 3 | Robo | Equipamiento IT, accesorios, software, datos, con información confidencial. |
| 5.5 | 5 | Vandalismo | Es como un ataque, interno y externo, pero no determinado por empleados frustados, clima de trabajo propicio. |
| 5.6 | 4 | Ataques | Sobre los operadores IT. |
| 5.7 | 3 | Intercepción de líneas | Existencia de programas debug de archivos que se pueden usar para otras cosas. |
| 5.8 | 3 | Uso no autorizado de sistemas IT | Sin identificación y autenticación no se puede controlar el uso no autorizado. Elección de contraseñas. Uso de diccionarios para romperlas. |
| 5.9 | 1 | Intercepción de llamadas telefónicas y transmisiones de datos | Por conferencia oculta o intercepción de línea. |
| 5.10 | 1 | Escuchas furtivas de salas | Terminales con micrófonos o uso del handsfree. |
| 5.11 | 2 | Mal uso de los derechos del administrador | Cuando se usan los privilegios del root de Unix para dañar el sistema o los usuarios. Puede ser con archivos con root como propietario y el bit seteado, o por medio del comando su. |
| 5.12 | 3 | Caballos de Troya | Funciones escondidas sin documentar. Cualquier programa más archivos batch, secuencias de control que sean interpretados por OS o aplicaciones. |
| 5.13 | 4 | Virus de computador | Puede destruir datos. De buteo, de archivos y macro virus. |
| 5.14 | 1 | Copia no autorizada de medios de datos | Puede ocurrir cuando se lo reemplaza o transporta que se han copias. |
| 5.15 | 1 | Uso no autorizado de máquinas de fax | Que usen papel con membrete de la empresa para cualquier uso particular o dañino para la empresa. |
| 5.16 | 1 | Visualización no autorizada de mensajes de fax entrantes | Si están en lugar abierto, cualquiera podría leer un mensaje que entra. |
| 5.17 | 3 | Ingeniería social | Generalmente mediante llamadas telefónicas haciéndose pasar por otros empleados o secretarias de jefes, o administradores para solucionar posibles errores. Hasta se puede usar para saber si una persona no estará por unos días y así intentar usar su cuenta. |
| 5.18 | 3 | Macro virus | Vienen con archivos de Word o Excel. Se ejecutan al cargar el archivo. |
| 5.19 | 4 | Falsificación de dirección IP | Usado para ataques indirectos por medio de intermediarios con la dirección de origen falsificada como si proviniera de otro usuario de modo que las respuestas múltiples irán a la dirección de la víctima. |

**Cuadro 17 (Continuación)**

| | | | |
|---|---|---|---|
| 5.20 | 3 | Abuso del protocolo ICMP | Por ser el ICMP un protocolo para información de errores y diagnóstico puede ser manipulado indebidamente por un hacker. |
| 5.21 | 4 | Mal uso de los derechos de administrador en sistemas Windows NT | Puede asumir propiedad de cualquier archivo. Podrían que quede registrado hace back up en connivencia con los encargados del BU. Alteración de hora o seguimiento detallado de la actividad de usuario. |
| 5.22 | 3 | Manipulación de datos o software en sistemas de bases de datos | Provoca que los datos sean alterados o no puedan usarse por acción directa sobre los mismos o eliminación o modificación de archivos. |
| 5.23 | 3 | Conexión no autorizada de dispositivos de computación a una red. | Puede ocurrir conectándose al cableado de la red o directamente a las interfaces de dispositivos de interconexión. |
| 5.24 | 2 | Ejecución no autorizada de funciones de gestión de red. | Por medio del acceso a puertos administrativos de dispositivos de interconexión en forma local o remota. |
| 5.25 | 1 | Acceso no autorizado a componentes activos de red | Estos dispositivos tienen puerto serial RS 232 o USB lo que permite su administración. Así podría leerse su configuración y lo que puede deducirse de la misma. |
| 5.26 | 3 | Pérdida de confiabilidad en la información clasificada | Referida tanto a datos confidenciales tanto de la empresa como personales, así como también a la referida a contraseñas y certificados digitales. |
| 5.27 | 4 | Falsificación de DNS | Ataque que consiste en alterar las tablas de equivalencia de nombres de sitios o máquinas con sus respectivas direcciones IP. |
| 5.28 | 3 | Pérdida de integridad de información que debiera estar protegida. | Imposibilidad de lectura, o alteración de datos accidental o maliciosamente. |
| 5.29 | 3 | Adquisición no autorizada de derechos de administrador con Windows NT | Esta cuenta no puede eliminarse ni deshabilitarse por lo que no reacciona frente a sucesivos intentos de registro. Una administración remota pasará la contraseña lo que facilita su escaneado. También están en el registro y en archivos conocidos, así como en disquetes y cintas de backups. También se podría lograr agregar una cuenta al grupo administrador. |
| 5.30 | 1 | Sabotaje | Manipulación o daño de objetos. Robo de UPS. |

Utilizando las amenazas clasificadas, se procedió a realizar un cruce entre los activos y las amenazas visualizado en el cuadro 18. Es de destacar, que para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en la intención de hacer daño.

**Cuadro 18**

**Cruce de las amenazas Vs. Activos**

| Ame-nazas | Activos Primarios | | | | | | | | | | | | | | | | | | | | | | | | | Ame-nazas |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 2.1 | 2.2 | 2.31 | 2.32 | 2.33 | 2.34 | 2.4 | 3.1 | 3.2 | 4.1 | 4.2 | 4.3 | 4.4 | 4.5 | 5.1 | 5.2 | 5.3 | 6.1 | 7.1 | 7.2 | |
| **1.1** | | X | | | X | | | | | | | | | X | X | X | | | X | X | | | | | | X | **1.1** |
| **1.2** | X | | | | X | | | | | X | | | | X | X | X | | | X | X | | X | | | | X | **1.2** |
| **1.3** | | | | | | | X | X | | X | | X | | X | X | | | | X | | | X | | X | | | **1.3** |
| **1.4** | | | | | | | X | X | X | X | X | X | X | X | X | X | | | X | | | X | | X | | | **1.4** |
| **1.5** | | | | | | | X | X | X | X | X | X | | X | X | X | | | X | | | X | | X | | | **1.5** |
| **1.6** | | | | | | | | X | | X | | X | | X | X | X | | | X | | | X | | X | | | **1.6** |
| **1.7** | | | | | | | | X | | X | X | X | | X | X | X | | | X | | | X | | X | | | **1.7** |
| **1.8** | X | X | | | | | | X | X | X | X | X | | X | X | X | | | X | | | X | | X | | | **1.8** |
| **1.9** | X | | X | | | | X | X | X | X | X | X | | X | X | X | | | X | | | X | | X | | | **1.9** |
| **1.10** | | | | | | | X | X | X | X | X | X | X | X | X | X | | | X | | | X | | X | | | **1.10** |
| **2.1** | X | | X | X | X | X | | X | | X | X | X | | X | X | X | | | X | X | X | | | | X | | **2.1** |
| **2.2** | | | X | X | | X | | | | X | | | | | | | | | | | | | | | | X | **2.2** |
| **2.3** | | | | | | | | | | | | | | | | | | | | | | | | | X | X | **2.3** |
| **2.4** | | | X | X | X | X | | | | X | X | | | | | X | | | | | | | | | | | **2.4** |
| **2.5** | | | X | | | X | | | | | | | | X | X | | | | | | | | | X | | X | **2.5** |
| **2.6** | | | | | | X | | X | | | X | | | X | X | | | | X | | X | | | | | X | **2.6** |
| **2.7** | | | | | | | | | | | | | | X | X | X | | | | | | | | | | X | **2.7** |
| **2.8** | | | X | | | X | | | | | | | | | | | | | | | | | | | | | **2.8** |
| **2.9** | | | | | | | | | | | | | | | | | | | | | X | | | | | X | **2.9** |
| **2.10** | | | | | | X | | | | X | X | X | | | | | | | | X | | | | | | | **2.10** |
| **2.11** | | | | | | | | X | | X | | X | | | | | | | | X | | | | | | | **2.11** |
| **2.12** | | | X | | | | | | | | X | X | | X | X | X | | | X | | | | | X | | X | **2.12** |
| **2.13** | | | | X | | | | | | | | | | X | | | | | | | | | | | | | **2.13** |
| **2.14** | | | | | | | | | | | X | | | | | | | | | | X | | | | | | **2.14** |
| **2.15** | | | X | | | | | | | | | | | | | | | | | | X | | | | | | **2.15** |
| **2.16** | | | | | X | | | | | | | | | | | | | | | | X | | | X | | | **2.16** |

**Cuadro 18 (Continuación)**

| Ame-nazas | ----------Activos Primarios---------- | | | | | | | | | | | | | | | | | | | | | | | | | Ame-nazas |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 2.1 | 2.2 | 2.31 | 2.32 | 2.33 | 2.34 | 2.4 | 3.1 | 3.2 | 4.1 | 4.2 | 4.3 | 4.4 | 4.5 | 5.1 | 5.2 | 5.3 | 6.1 | 7.1 | 7.2 | |
| **2.17** | | | | | | | | | | | | | | | | | X | | | | | | X | | | X | **2.17** |
| **2.18** | | | | | | | | | | | | | | | | | | X | | | | | | | X | X | **2.18** |
| **2.19** | | | X | | | X | | | | | | | | | | | | | | X | | | | | X | X | **2.19** |
| **2.20** | | | | | | | | | | | | | | | | | | | | X | | | | | X | X | **2.20** |
| **2.21** | | | X | | | | | | | | | | | | | | | | | X | X | | | | X | X | **2.21** |
| **2.22** | | | | | | X | | | | | | | | | | | | | | X | | | | | | X | **2.22** |
| **2.23** | | | | | | | | | | | | | | X | X | X | | X | | | | | | | | | **2.23** |
| **2.24** | | | | | | | | | | | | | | X | X | X | | X | | | | | | | | X | **2.24** |
| **2.25** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **2.25** |
| **2.26** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **2.26** |
| **2.27** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **2.27** |
| **2.28** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **2.28** |
| **2.29** | | | | | | | | | | | | | | | | X | | | X | X | | | | | | X | **2.29** |
| **2.30** | | | X | | | | | | | | X | | | | | | | | | | | | | | | X | **2.30** |
| **2.31** | | | X | | | | | | | | | | | | | | | | | | X | | | | | X | **2.31** |
| **2.32** | | | | X | | | | | | | | | | | | | | | | X | X | | | | | | **2.32** |
| **2.33** | | | | | | X | | | | | X | | | | | X | | | X | X | X | | | | | X | **2.33** |
| **2.34** | | | | | | | | | | | | | | | | | | | | X | X | | | | | X | **2.34** |
| **2.35** | | | | | | | | | | | | | X | | | | | | | | | | | | | | **2.35** |
| **3.1** | | | | | X | | | | | | | | | | | | | | | X | X | | | | | X | **3.1** |
| **3.2** | | | | | X | | | | | | | | | | X | X | | | X | | | | | | | X | **3.2** |
| **3.3** | | | | | X | | | | | | X | X | | X | X | X | | | X | | | | | | X | X | **3.3** |
| **3.4** | | | | | | | | | | | | | | | | | | | | | X | | | | | | **3.4** |
| **3.5** | | | | | | | | X | | | | | | X | X | X | | | X | | | | | | | X | **3.5** |
| **3.6** | | | | | X | | | | | | X | | | X | X | | | | | X | | | | | | | **3.6** |
| **3.7** | | | X | X | | X | | | | | X | | | X | X | | | | | X | | | | | | X | **3.7** |
| **3.8** | | | | | | | | | | | | | | | | | | | | X | | | | | | X | **3.8** |
| **3.9** | | | | | | | | | | | | | | | | | | | | | X | | | | | X | **3.9** |
| **3.10** | | | | | | | | | | | | | | | | | X | | | | | | X | | | | **3.10** |

**Cuadro 18 (Continuación)**

| Ame-nazas | ----------Activos Primarios---------- | | | | | | | | | | | | | | | | | | | | | | | | | Ame-nazas |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 2.1 | 2.2 | 2.31 | 2.32 | 2.33 | 2.34 | 2.4 | 3.1 | 3.2 | 4.1 | 4.2 | 4.3 | 4.4 | 4.5 | 5.1 | 5.2 | 5.3 | 6.1 | 7.1 | 7.2 | |
| **3.11** | | | | | | | | | | | | | | | | | X | | | | | | X | | | | **3.11** |
| **3.12** | | | | | | | | | | | X | | | | | | | | | X | | | | | | X | **3.12** |
| **3.13** | | | | | | | | | | | | | | | | | | | | X | X | | | | | X | **3.13** |
| **3.14** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **3.14** |
| **3.15** | | | | | | | | | | | | | | | | | | | X | X | | | | | | X | **3.15** |
| **3.16** | | | | | | | | | | | | | | | | | | | | X | | | | | | X | **3.16** |
| **3.17** | | | | | | | | | | | | | | X | X | X | | | | | | | | | X | X | **3.17** |
| **3.18** | | | X | X | | | | | | | X | | | X | X | X | | | X | | | | | | | X | **3.18** |
| **3.19** | | | | | | | | | | | | | | X | X | X | | | | | | | | | | X | **3.19** |
| **4.1** | | | X | | X | | | | | X | | | | X | X | X | X | | X | | | X | X | X | | | **4.1** |
| **4.2** | | | | | | | | | | X | | | | X | X | X | | | X | | | X | | X | | | **4.2** |
| **4.3** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **4.3** |
| **4.4** | | | | | | | | | | | | | | | | | | | | | | | | | X | X | **4.4** |
| **4.5** | | | | | | | | | | | X | | | | | | | X | | | X | | | | | | **4.5** |
| **4.6** | | | | | | | | | | | | | | | | | | | | | X | | | | | | **4.6** |
| **4.7** | | | | | X | | | | | | | | | | | | | | | | X | | | | | | **4.7** |
| **4.8** | | | X | | | | | | | | | | | | | | | | | | | | | | | X | **4.8** |
| **4.9** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **4.9** |
| **4.10** | | | X | | | | | | | | | | | | | | | | | | | | | | | X | **4.10** |
| **4.11** | | | X | | | | | | | | | | | | | | | | | | | | | | | X | **4.11** |
| **4.12** | | | | | | | | | | | | | | X | X | X | | | X | | | | | | | X | **4.12** |
| **4.13** | | | | | | | | | | | | | | | | | X | | | | | | X | | | X | **4.13** |
| **4.14** | | | | | | | | | | | | | | | | | | | | | | | | | X | | **4.14** |
| **4.15** | | | | | | | | | | | | | | | | | | | | | | | | | | | **4.15** |

**Cuadro 18 (Continuación)**

| Ame-nazas | ----------Activos Primarios---------- | | | | | | | | | | | | | | | | | | | | | | | | | Ame-nazas |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 2.1 | 2.2 | 2.31 | 2.32 | 2.33 | 2.34 | 2.4 | 3.1 | 3.2 | 4.1 | 4.2 | 4.3 | 4.4 | 4.5 | 5.1 | 5.2 | 5.3 | 6.1 | 7.1 | 7.2 | |
| **4.16** | | | | | | | | | | | | | | | | | | X | | | | | | | | | **4.16** |
| **5.1** | | | X | | X | | | | | | | | | X | X | X | | | X | | | | | | | X | **5.1** |
| **5.2** | | | | | X | | | | | | | | | | | | | | | | | | | | | X | **5.2** |
| **5.3** | | | | | | | | | | | X | | | X | X | X | | | X | | | X | | X | | X | **5.3** |
| **5.4** | X | | | | | | | | X | X | X | X | | X | X | X | | | X | | | | | X | | | **5.4** |
| **5.5** | X | | | | X | | X | X | X | X | X | X | X | X | X | X | | | X | | | X | | X | | | **5.5** |
| **5.6** | X | X | | | X | | | | | | | | | X | X | X | | | X | | | | | | | X | **5.6** |
| **5.7** | | | | | | | | | | | X | | | X | X | X | | | | | | | | | | X | **5.7** |
| **5.8** | | | | | | | | | | | | | | X | X | X | | | | | | | | | | X | **5.8** |
| **5.9** | | | X | | X | | | | | | X | | | | | | | | | | | | | | | | **5.9** |
| **5.10** | | | | | X | | | | | | | | | | | | | | | | | | | | | | **5.10** |
| **5.11** | X | | X | | X | | | | | | | | | X | X | X | | | X | | | | | | | X | **5.11** |
| **5.12** | | | X | X | | | | | | | | | | X | X | X | | | | | | | | | X | X | **5.12** |
| **5.13** | | | X | X | X | | | | | | | | | X | X | X | | X | | | | | | | X | | **5.13** |
| **5.14** | | | X | | X | | | | | | X | | | | | | | | | | | | | | | X | **5.14** |
| **5.15** | X | | | | | | | | | | | | | | | | | | | | | | | | | | **5.15** |
| **5.16** | | | | | X | | | | | | | | | | | | | | | | | | | | | | **5.16** |
| **5.17** | | | | | X | | | | | | X | | | | | | | | | | | | | | | X | **5.17** |
| **5.18** | | | X | X | X | | | | | | | | | X | X | X | | X | | | | | | | X | X | **5.18** |
| **5.19** | | | | | | | | | | | | | | X | X | X | | | | | | | | | | X | **5.19** |
| **5.20** | | | | | | | | | | | | | | | | X | | | X | | | | | | | X | **5.20** |
| **5.21** | | | | | | | | | | | | | | | | | | X | | | | | | | | | **5.21** |
| **5.22** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **5.22** |
| **5.23** | | | | | X | | | | | | | | | | | | | | | | | | | | | X | **5.23** |
| **5.24** | | | | | | | | | | | | | | | | X | | | X | | | | | | | X | **5.24** |
| **5.25** | | | | | | | | | | | | | | | | X | | | X | | | | | | | | **5.25** |
| **5.26** | | | | | X | | | | | | | | | | | | | | | | | | | | | X | **5.26** |

**Cuadro 18 (Continuación)**

| Ame-nazas | ----------Activos Primarios---------- | | | | | | | | | | | | | | | | | | | | | | | | | Ame-nazas |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 2.1 | 2.2 | 2.31 | 2.32 | 2.33 | 2.34 | 2.4 | 3.1 | 3.2 | 4.1 | 4.2 | 4.3 | 4.4 | 4.5 | 5.1 | 5.2 | 5.3 | 6.1 | 7.1 | 7.2 | |
| **5.27** | | | | | | | | | | | | | | | | | | | | | | | | | | X | **5.27** |
| **5.28** | | | | | X | | | | | | X | | | | | | | | | | | | | | | X | **5.28** |
| **5.29** | X | X | X | X | | | | | X | X | X | X | | X | X | X | | X | X | X | | | | X | | X | **5.29** |
| **5.30** | | | | | | | | | | | | | | | | | | | | | | | | | | | **5.30** |

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización. Al respecto, Peltier (2001), define la vulnerabilidad como una debilidad en el sistema, aplicación o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema. Es de destacar, que las vulnerabilidades no causan daño, simplemente son condiciones que pueden hacer que una amenaza afecte un activo. En el cuadro 19, se presenta algunas vulnerabilidades clasificadas en tipo 1: física, organizacionales y operacionales, tipo 2: técnica para plataforma Windows, tipo 3: técnica para plataforma Linux y tipo 4: técnica de otros dispositivos.

**Cuadro 19**

**Vulnerabilidades clasificadas**

| VULNERABILIDADES CLASIFICADAS | | |
|---|---|---|
| TIPO 1 - FISICAS, ORGANIZACIONALES Y OPERACIONALES | | |
| **Nro.** | **Nivel** | **Descripción** |
| **1.1** | | **SEGURIDAD LOGICA** |
| **1.1.1** | | **Identificación** |
| 1.1.1.1 | 1 | Datos del perfil de usuarios dados de alta |
| 1.1.1.2 | 2 | Gestión de bajas de usuarios |
| 1.1.1.3 | 2 | Mantenimiento de cuentas |
| 1.1.1.4 | 2 | Manejo de los permisos para los accesos |
| 1.1.1.6 | 1 | Identificación única o grupal |
| 1.1.1.7 | 1 | Gestión de grupos |
| 1.1.1.8 | 2 | Súper usuario |
| 1.1.1.9 | 1 | Visualización del logeo en pantalla |
| **1.1.2** | | **Autenticación** |
| 1.1.2.1 | 2 | Manejo de los datos de autenticación |
| 1.1.2.2 | 1 | Manejo de intentos de logeo |
| **1.1.3** | | **Contraseñas** |
| 1.1.3.1 | 2 | Generación de contraseñas |
| 1.1.3.2 | 1 | Gestión de cambio de contraseñas |
| **1.1.4** | | **Control de acceso lógico** |
| 1.1.4.1 | 1 | Modelo y aplicación |
| 1.1.4.2 | 2 | Criterios de acceso |
| 1.1.4.3 | 3 | Mecanismos de control de acceso interno |
| 1.1.4.4 | 3 | Control de acceso externo |
| **1.2** | | **SEGURIDAD EN LAS COMUNICACIONES** |
| **1.2.1** | | **Configuración de la red** |
| 1.2.1.1 | 3 | Comunicaciones vía modem |
| 1.2.1.2 | 2 | Recursos compartidos de discos de PC |
| 1.2.1.3 | 1 | Estado de puertos de servicios no necesarios |

**Cuadro 19 (Continuación)**

| VULNERABILIDADES CLASIFICADAS | | |
|---|---|---|
| **1.2.2** | | **Virus y Antivirus** |
| 1.2.2.1 | 3 | No está habilitado para envío y recepción de mail |
| 1.2.2.2 | 2 | Actualizaciones no adecuadamente frecuentes |
| 1.2.2.3 | 2 | No es suficiente la frecuencia de escaneado de las unidades de las computadores |
| 1.2.2.4 | 1 | No se generan discos de rescate en las PCs bajo Win |
| **1.2.3** | | **Documentación, normas** |
| 1.2.3.1 | 1 | Grado y detalle de la información documentada de la red |
| 1.2.3.2 | 2 | Gestión y procesos de parches |
| 1.2.3.3 | 1 | Documentación de la configuración de las PCs |
| **1.2.4** | | **Ataques a la red** |
| 1.2.4.1 | 1 | Antecedentes de ataques ocurridos a la red |
| **1.2.5** | | **Firewall** |
| 1.2.5.1 | 3 | Tipo, configuración y nivel de control de firewall |
| 1.2.5.2 | 1 | Pruebas de configuración de firewall |
| **1.2.5** | | **Máquinas de Fax** |
| 1.2.5.1 | 2 | Control de envíos por fax |
| 1.2.5.2 | 1 | Distribución de faxes recibidos |
| **1.3** | | **SEGURIDAD EN LAS APLICACIONES** |
| **1.3.1** | | **Sistema Operativo** |
| 1.3.1.1 | 1 | Requisitos de seguridad considerados al elegir el sistema operativo |
| **1.3.2** | | **Control de datos de aplicaciones** |
| 1.3.2.1 | 1 | Existencia de control de cambios para archivos de sistema o bases de datos |
| 1.3.2.2 | 3 | Confidencialidad de datos de laptops y notebooks |
| 1.3.2.3 | 2 | Logs de transacciones y sus detalles |
| **1.3.3** | | **Control de datos en el desarrollo** |
| 1.3.3.1 | 1 | Existencia de control de cambios para el desarrollo |
| 1.3.3.2 | 1 | Control del contenido de archivos de entrada |
| 1.3.3.3 | 2 | Control de validez de datos ingresados manualmente |
| 1.3.3.4 | 1 | Control de consistencia de datos de salida |
| **1.3.4** | | **Seguridad de bases de datos** |
| 1.3.4.1 | 2 | Control de acceso propio de las bases de datos |
| 1.3.4.2 | 1 | Control de instancias de uso |
| 1.3.4.3 | 1 | Chequeo regulares de seguridad |
| 1.3.4.4 | 1 | Marcado o borrado de archivos eliminados |
| **1.3.5** | | **Control de aplicaciones** |
| 1.3.5.1 | 2 | Controles con que se realiza la instalación y actualización de parches |
| 1.3.5.2 | 1 | Documentación de la instalación o actualización de software |
| 1.3.5.3 | 2 | Control de aplicaciones en máquinas de usuarios |
| 1.3.5.4 | 1 | Control de información que bajan los usuarios de la Web |
| **1.3.6** | | **Mantenimiento de aplicaciones** |
| 1.3.6.1 | 1 | Documentación de cambios de emergencia |
| 1.3.6.2 | 1 | Control regular de programas y servicios innecesarios |
| 1.3.6.3 | 1 | Gestión de cambios complejos en archivos de configuración |
| 1.3.6.4 | 2 | Registro de cambios en las configuraciones |

**Cuadro 19 (Continuación)**

| VULNERABILIDADES CLASIFICADAS | | |
|---|---|---|
| **1.3.7** | | **Ciclo de vida** |
| 1.3.7.1 | 1 | Metodología usada para el desarrollo |
| 1.3.7.2 | 2 | Manejo del código fuente y documentación con desarrollos por terceros |
| 1.3.7.3 | 1 | Uso métricas en el desarrollo |
| 1.3.7.4 | 1 | Registros históricos de las modificaciones |
| 1.3.7.5 | 2 | Existencia de requisitos de seguridad |
| 1.3.7.6 | 1 | Medidas de seguridad durante las implementaciones |
| 1.3.7.7 | 1 | Forma y documentación de pruebas |
| 1.3.7.8 | 1 | Metodología usada para el mantenimiento |
| 1.3.7.9 | 1 | Detalles de la documentación generada en el desarrollo |
| **1.4** | | **SEGURIDAD FISICA** |
| **1.4.1** | | **Control de acceso al centro de cómputos** |
| 1.4.1.1 | 2 | Restricción de acceso a personas ajenas al área |
| 1.4.1.2 | 1 | Control personal de limpieza en locales con servidores |
| **1.4.2** | | **Control de acceso a los equipos de los usuarios** |
| 1.4.2.1 | 2 | Habilitación del NetBIOS |
| 1.4.2.2 | 1 | Habilitación y control de dispositivos externos |
| 1.4.2.3 | 3 | Control de virus |
| 1.4.2.4 | 2 | Existencia de grabadoras de CD |
| 1.4.2.5 | 1 | Agregado no autorizado de dispositivos externos |
| 1.4.2.6 | 2 | Control y revisión de dispositivos instalados en las PCs |
| 1.4.2.7 | 1 | Apagado o no de los servidores |
| **1.4.3** | | **Utilidades de soporte** |
| 1.4.3.1 | 2 | Gestión de fallas dispositivos externos al funcionamiento del equipamiento IT |
| **1.4.4** | | **Estructura del edificio** |
| 1.4.4.1 | 1 | Tipo, condiciones e instalación del cableado de red |
| 1.4.4.2 | 1 | Falta de información de otras instalaciones que corran en paralelo |
| 1.4.4.3 | 1 | Actividades que pueden afectar las operaciones |
| 1.4.4.4 | 1 | Actividades externas que pueden afectar las operaciones |
| 1.4.4.5 | 2 | Protecciones antirrayos |
| **1.4.5** | | **Clasificación de datos y hardware** |
| 1.4.5.1 | 1 | Forma de rotular computadoras y periféricos |
| 1.4.5.2 | 1 | Inventario de recursos de hardware y software |
| **1.4.6** | | **Backup** |
| 1.4.6.1 | 2 | Frecuencia de backups |
| 1.4.6.2 | 2 | Datos que se backapean |
| 1.4.6.3 | 2 | Tipos de backup que se realizan |
| 1.4.6.4 | 2 | Medios de almacenamiento de backups |
| 1.4.6.5 | 1 | Rotación de medios |
| 1.4.6.6 | 1 | Herramientas de backup |
| 1.4.6.7 | 2 | Responsables del backup |
| 1.4.6.8 | 1 | Procedimientos de backup |
| 1.4.6.9 | 2 | Pruebas periódicas de recuperación |

**Cuadro 19 (Continuación)**

| VULNERABILIDADES CLASIFICADAS | | |
|---|---|---|
| 1.4.6.10 | 2 | Lugar de almacenamiento y controles de acceso |
| 1.4.6.11 | 1 | Rotulación y documentación de backups |
| **1.5** | | **ADMINISTRACION DEL CENTRO DE COMPUTOS** |
| **1.5.1** | | **Contramedidas** |
| 1.5.1.1 | 1 | Tipo y regularidad de chequeos |
| 1.5.1.2 | 2 | Planificación y documentación de actividades del área |
| 1.5.1.3 | 1 | Documentación detallada del equipamiento |
| 1.5.1.4 | 2 | Documentación y manuales de procedimientos y seguridad |
| **1.5.2** | | **Responsabilidad del equipo de seguridad** |
| 1.5.2.1 | 3 | Administración de emergencias |
| **1.6** | | **REGISTROS Y AUDITORIAS** |
| **1.6.1** | | **Auditorias generales** |
| 1.6.1.1 | 2 | Realización y objetos auditados |
| 1.6.1.2 | 1 | Monitoreo y herramientas |
| 1.6.1.3 | 2 | Gestión de logs |
| 1.6.1.4 | 1 | Utilidad auditoría para rastreo de acciones |
| 1.6.1.5 | 1 | Históricos generados |
| **1.6.2** | | **Logs** |
| 1.6.2.1 | 3 | Control de acceso |
| 1.6.2.2 | 2 | Identificación y almacenamiento |
| 1.6.2.3 | 2 | Información contenida en los logs |
| 1.6.2.4 | 1 | Análisis que se realiza |
| **1.6.3** | | **Auditoría de servidores** |
| 1.6.3.1 | 1 | Trabajos de mayor uso CPU y memoria |
| 1.6.3.2 | 1 | Datos de mayor tráfico, CPU y memoria |
| 1.6.3.3 | 1 | Aplicaciones de mayor tráfico, CPU y memoria |
| **1.6.4** | | **Auditoría de control de acceso** |
| 1.6.4.1 | 2 | Existencia de logs |
| 1.6.4.2 | 2 | Almacenamiento y acceso |
| 1.6.4.3 | 1 | Duración y tratamiento posterior al vencimiento |
| 1.6.4.4 | 2 | Contenido de los logs |
| **1.6.5** | | **Auditoría de redes** |
| 1.6.5.1 | 1 | Monitoreo de red |
| 1.6.5.2 | 1 | Periodicidad de chequeos |
| 1.6.5.3 | 1 | Datos revisados y estadísticas |
| **1.7** | | **PLAN DE CONTINGENCIAS** |
| **1.7.1** | | **Plan de contingencias** |
| 1.7.1.1 | 2 | Existencia, justificaciones |
| 1.7.1.2 | 1 | Alcance del plan |
| 1.7.1.3 | 2 | Responsabilidades y entrenamiento |
| 1.7.1.4 | 2 | Documentación |
| **1.7.2** | | **Plan de recuperación de desastres** |
| 1.7.2.1 | 3 | Responsabilidades |
| 1.7.2.2 | 2 | Identificación de funciones críticas |

**Cuadro 19 (Continuación)**

| VULNERABILIDADES CLASIFICADAS | | |
|---|---|---|
| 1.7.2.3 | 2 | Grupo y responsable |
| 1.7.2.4 | 2 | Inventario de equipamiento |
| **1.7.3** | | **Administradores de aplicaciones y sistemas** |
| 1.7.3.1 | 1 | Personal de desarrollo |
| 1.7.3.2 | 2 | Técnicos |
| 1.7.3.3 | 2 | Administradores de Redes |
| **1.7.4** | | **Gerencia en seguridad** |
| 1.7.4.1 | 3 | Visón y compromiso general y medio en la seguridad |
| 1.7.4.2 | 3 | Reglas de seguridad |
| 1.7.4.3 | 1 | Personal en general - procedimientos |
| 1.7.4.4 | 2 | Personal de desarrollo - procedimientos |
| 1.7.4.5 | 3 | Técnicos - procedimientos |
| 1.7.4.6 | 3 | Administradores de redes - procedimientos |
| | | **TIPO 2 - TECNICAS DE PLATAFORMAS LINUX** |
| **2.1** | | **SERVICIOS ACTIVOS INNECESARIOS** |
| 2.1.1 | 2 | Hay habilitados servicios innecesarios |
| **2.2** | | **Bind/DNS** |
| 2.2.1 | 2 | Instalación/ISC, versión y parches |
| 2.2.2 | 2 | Actualización dinámica del DNS |
| 2.2.3 | 2 | Demonio named habilitado en servidores no DNS |
| **2.3** | | **RPC** |
| 2.3.1 | 3 | RPC Habilitado |
| 2.3.3 | 2 | Servicios RPC que se pueden explotar |
| **2.4** | | **SNMP** |
| 2.4.1 | 2 | Versión y puertos habilitados |
| 2.4.2 | 3 | Nombres comunidad por default |
| 2.4.3 | 2 | Chequeo registros MIB |
| **2.5** | | **Shell seguro** |
| 2.5.1 | 1 | Instalación y versión |
| **2.6** | | **Servicios NIS/NFS** |
| 2.6 .1 | 3 | Versión NIS |
| 2.6 .2 | 3 | Ubicación password del root con NIS |
| 2.6 .3 | 2 | Versión NFS |
| 2.6 .4 | 3 | Configuración archivo export y montaje de sistema de archivos NFS |
| **2.7** | | **Open SSL** |
| 2.7.1 | 1 | Versión |
| **2.8** | | **FTP** |
| 2.8.1 | 3 | Habilitación y funcionalidad anónima |
| 2.8.2 | 3 | Sin uso de password en el modo de subida |
| 2.8.3 | 3 | No hay restricciones y mecanismos para direcciones IP o dominios |
| 2.8.4 | 3 | No se usan restricciones propias del servidor ftp |
| 2.8.5 | 3 | Especificación de las cuentas administrativas en archivo ftpusers |
| 2.8.6 | 3 | No hay diferenciación archivos contraseñas con los del OS |
| 2.8.7 | 2 | Permisos y propietarios del raíz y subdirectorios etc y bin del ftp anónimo |

**Cuadro 19 (Continuación)**

| VULNERABILIDADES CLASIFICADAS | | |
|---|---|---|
| 2.8.8 | 2 | Permisos y propietarios de archivos de subdirectorios etc y bin |
| 2.8.9 | 2 | Permisos y propietarios directorio home ~ftp/ |
| 2.8.10 | 3 | Existencia de archivos .rhosts y .forward |
| 2.8.11 | 3 | Restricciones de escritura para everyone en directorios ftp y sus archivos |
| **2.9** | | **Otras de contraseñas** |
| 2.9.1 | 2 | Hay cuentas extras con UID 0, o sin contraseñas en el archivo passwd |
| 2.9.2 | 3 | tftp habilitado |
| 2.9.3 | 3 | tftp necesario pero sin precauciones de acceso restringido |
| 2.9.4 | 2 | No se usa un programa para mejorar la elección de contraseñas |
| **2.10** | | **Otros Servicios de red** |
| 2.10.1 | 2 | Permisos y propietarios no adecuados en archivos de servicios de red |
| 2.10.2 | 2 | Cron acepta usuarios ordinarios |
| 2.10.3 | 3 | Se puede registrar como root en la consola en forma remota |
| 2.10.4 | 3 | Terminales no adecuados en el archivo de terminal seguro |
| **2.11** | | **Seguridad sistema de archivos** |
| 2.11.1 | 2 | Archivos .exrc no justificados |
| 2.11.2 | 2 | Archivos .forward en directorios home de usuarios |
| 2.11.3 | 2 | Umask inadecuado de algunos programas |
| 2.11.4 | 2 | Restricciones de acceso no adecuadas en algunos archivos bajo /etc |
| 2.11.5 | 3 | Escritura indebida de los archivos log |
| 2.11.6 | 2 | Características extendidas (inmutabilidad y sólo anexado) no habilitadas |
| 2.11.7 | 2 | Inadecuados permisos, propiedad y grupo de /vmunix |
| 2.11.8 | 3 | Archivos que no debieran ser propiedad sino de root, y si /tmp no tiene el sticky-bit |
| 2.11.9 | 3 | Archivos o directorios no esperados que son escribibles por cualquiera |
| 2.11.10 | 2 | Archivos que no debieran tener seteados el bit SUID o SGID |
| 2.11.11 | 2 | Umask inadecuado de algunos usuarios |
| 2.11.12 | 2 | Archivos ordinarios en el directorio /dev |
| 2.11.13 | 2 | Archivos especiales fuera de /dev |
| 2.11.14 | 2 | Archivos ejecutables y sus directorios ascendentes escribibles por grupos o cualquiera |
| 2.11.15 | 2 | Archivos sin propietarios |
| **2.12** | | **Monitoreo del sistema** |
| 2.12.1 | 3 | No se han definido los archivos log adecuados para seguridad |
| 2.12.2 | 2 | No se usan las extensiones de seguridad de Linux para los archivos log |
| 2.12.3 | 3 | Ausencia de registro de las actividades de los administradores |
| 2.12.4 | 2 | Falta de control de las modificaciones de archivos de sistema |
| **2.13** | | **Servicios de archivos** |
| 2.13.1 | 2 | Inadecuados permisos y propiedad del archivo /etc/export |
| **2.14** | | **Linux** |
| 2.14.1 | 3 | Parches y actualizaciones |
| | | **Tipo 3 - TECNICAS DE PLATAFORMAS WINDOWS XP/2003** |
| **3.1** | | **IIS** |
| 3.1.1 | 3 | Versión y parches del IIS |
| 3.1.2 | 2 | Versiones 4 y 5 del IIS; ACL y directorios |
| 3.1.3 | 2 | Habilitación del log del IIS |

**Cuadro 19 (Continuación)**

| VULNERABILIDADES CLASIFICADAS | | |
|---|---|---|
| 3.1.4 | 3 | WebDav ntdll.dll en IIS 5.0 |
| 3.1.5 | 2 | Aplicaciones de muestra en directorios iissamples, iishelp y msadc |
| **3.2** | | **SQL Server** |
| 3.2.1 | 3 | Versión y parches del SQL Server |
| 3.2.2 | 2 | Log autenticación servidor SQL |
| 3.2.3 | 2 | Cuenta SA, contraseña |
| **3.3** | | **Autenticación** |
| 3.3.1 | 3 | Autenticación, algoritmo usado |
| 3.3.2 | 3 | Archivo hashes LM, habilitación autenticación a través de la red |
| **3.4** | | **Internet Explorer** |
| 3.4.1 | 3 | Versión y parches del Internet Explorer |
| 3.4.2 | 2 | Nivel seguridad del IE |
| **3.5** | | **RAS** |
| 3.5.1 | 3 | Uso SMB, conectividad NetBios |
| 3.5.2 | 2 | Sesión nula, registro anónimo |
| 3.5.3 | 3 | Acceso remoto al registry |
| 3.5.4 | 3 | rpc y parches |
| **3.6** | | **MDAC/RDS** |
| 3.6.1 | 3 | Versión y parches del MDAC |
| 3.6.2 | 2 | Archivo msadcs.dll con NT 4.0 e IIS 3.0 o 4.0 |
| 3.6.3 | 1 | Versión y SP del Jet Engine |
| **3.7** | | **Windows Scripting Host** |
| 3.7.1 | 3 | Habilitación del Windows Scripting Host |
| 3.7.2 | 1 | Forma de ejecución de scripts |
| **3.8** | | **Outlook Express** |
| 3.8.1 | 2 | Ventana de vista previa del Outlook/Outlook Express |
| 3.8.2 | 1 | Restricción zona de seguridad del Outlook Express |
| **3.9** | | **Compartición P2P** |
| 3.9.1. | 3 | Puertos de aplicaciones P2P |
| 3.9.2 | 2 | Existencia en disco de archivos propios de P2P |
| **3.10** | | **SNMP** |
| 3.10.1 | 2 | Versión y puertos habilitados del SNMP |
| 3.10.2 | 3 | Nombres comunidad por default del SNMP |
| 3.10.3 | 2 | Chequeo registros MIB del SNMP |
| **3.11** | | **Acceso remoto al registry** |
| 3.11.1 | 3 | Registros bajo SecurePipeServers |
| **3.12** | | **Otros seteados del registry** |
| 3.12.1 | 3 | Registro Winlogon |
| 3.12.2 | 2 | Registro LanMan Print Services, para no poder agregar drivers impresión |
| 3.12.3 | 2 | Registro Subsystems, OS/2 y Posix |
| 3.12.4 | 2 | Registro bajo EventLog, para que no se vean los logs de aplicaciones y sistema |
| 3.12.5 | 2 | Registro Session Manager, atributos recursos compartidos, borrado archivo páginas |

**Cuadro 19 (Continuación)**

| VULNERABILIDADES CLASIFICADAS | | |
|---|---|---|
| **3.14** | | **Otras cuestiones de contraseñas** |
| 3.14.1 | 2 | Uso del passfilt.dll |
| 3.14.2 | 1 | Uso del syskey.exe |
| **3.15** | | **Sistema de archivos** |
| 3.15.1 | 3 | Se usa FAT |
| 3.15.2 | 2 | Grupos Everyone (Todos) y/o Usuarios controlados |
| **3.16** | | **Logs de auditoria** |
| 3.16.1 | 2 | Logs en Event Viewer |
| 3.16.2 | 1 | Nombres existentes en registro HKLM\System\CurentControlSer\\Control\Lsa |
| **3.17** | | **Utilitarios de cuidado** |
| 3.17.1 | 2 | Existencia y/o restricciones de acceso de archivos ejecutables de cuidado |
| 3.17.2 | 1 | Ubicación de los archivos ejecutables de cuidado |
| 3.17.3 | 2 | Existencia del programa rollback.exe |
| **3.18** | | **Subsistemas de cuidado** |
| 3.18.1 | 2 | Existencia de c:\winnt\system32\os2 y subdirectorios |
| 3.18.2 | 2 | Archivos del os2 y posix en c:\winnt\system32 |
| 3.18.3 | 1 | Registros os2 subsystem for nt |
| | | **Tipo 4 - TECNICAS DE OTROS DISPOSITIVOS** |
| **4.1** | 2 | **Grupos de PCs** |
| **4.2** | 3 | **Grupos de laptops y notebooks** |
| **4.3** | 3 | **Routers** |
| **4.4** | 3 | **Switches** |
| **4.5** | 2 | **Otros dispositivos** |

Con las vulnerabilidades clasificadas se procedió a verificar cada una de ellas con los activos del SGSI, (ver anexo I), a continuación se presentan el resumen.

**Cuadro 20**

Resumen de las vulnerabilidades para el Sistema Administrativo Integrado SAI

| | | | Plataforma Windows | | | |
|---|---|---|---|---|---|---|
| | **Vulnerabilidades Físicas, Organizacionales y Operacionales** | **Plataforma Linux Firewall** | **SAI** | **Prestaciones** | **Nomina** | **DNS, DHCP, Active Directory** |
| Total de vulnerabilidades potenciales | 109 | 55 | 43 | 43 | 43 | 43 |
| Vulnerabilidades no presente | 5 | 4 | 0 | 14 | 12 | 13 |
| Vulnerabilidades de nivel 1 | 55 | 2 | 6 | 3 | 4 | 4 |
| Vulnerabilidades de nivel 2 | 42 | 28 | 21 | 16 | 17 | 15 |
| Vulnerabilidades de nivel 3 | 7 | 21 | 16 | 10 | 10 | 11 |
| Nivel Relativo de Vulnerabilidad Total | 160 | 65 | 96 | 65 | 68 | 67 |
| Servidores más vulnerables | | | *** | | *** | |
| Servidores más vulnerable en el Nivel 3 | | *** | *** | | | |

Autora: 2007

*Calculo de las Amenazas y Vulnerabilidades*

Una vez identificadas las amenazas y vulnerabilidades, es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo. Al respecto, Peltier (ob. cit.) define el riesgo como la probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular. A continuación se presentan los cruces de las amenazas y vulnerabilidades para obtener el nivel de riesgo de los activos más importantes del Sistema Administrativo Integrado, como son: sala de servidores, software y aplicaciones, servidores en plataforma Windows y Linux (SAI, Firewall, DNS, DHCP y Active Directory).

## Cuadro 21

Cruce de las Amenazas y las Vulnerabilidades de la Sala de Servidores (Activo 2.32)

| Nro. | Niv. | Amenazas Descripción | Vulnerabilidades | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1.2 | 4 | Fallas de los sistemas IT | 1.7.1.1 | 1.7.1.2 | 1.7.1.3 | 1.7.1.4 | 1.7.2.1 | 1.7.2.2 | 1.7.2.3 | 1.7.2.4 |
| 1.3 | 2 | Rayos | 1.4.4.5 | | | | | | | |
| 1.4 | 4 | Incendio | 1.4.3.1 | | | | | | | |
| 1.5 | 3 | Inundación | 1.4.4.2 | | | | | | | |
| 1.6 | 2 | Cables quemados | 1.4.3.1 | | | | | | | |
| 1.7 | 2 | Polvo y suciedad | 1.4.4.3 | | | | | | | |
| 1.8 | 2 | Efectos de catástrofes en el ambiente | 1.4.4.4 | | | | | | | |
| 1.9 | 2 | Problemas causados por grandes eventos públicos | 1.4.4.4 | | | | | | | |
| 1.10 | 2 | Tormentas | 1.4.4.4 | | | | | | | |
| 2.1 | 4 | Falta o insuficiencia de reglas de seguridad en general | 1.2.3.1 | 1.2.4.1 | 1.5.1.4 | | | | | |
| 2.2 | 5 | Conocimiento insuficiente de documentos sobre reglas y procedimientos | 1.5.2.1 | | | | | | | |
| 2.4 | 3 | Monitoreo insuficiente de las medidas de seguridad IT | 1.6.1.1 | 1.6.1.2 | 1.6.1.3 | 1.6.1.4 | 1.6.1.5 | | | |
| 2.10 | 3 | Dimensionamiento insuficiente de redes y centro de cómputo | 1.5.1.1 | | | | | | | |
| 2.11 | 2 | Documentación insuficiente del cableado | 1.4.4.1 | | | | | | | |
| 5.4 | 3 | Robo | 1.4.1.1 | | | | | | | |
| 5.5 | 5 | Vandalismo | 1.4.4.3 | 1.4.4.4 | | | | | | |
| 5.29 | 1 | Sabotaje | 1.4.1.1 | 1.4.1.2 | 1.4.4.3 | 1.4.4.4 | | | | |

## Cuadro 22

Vulnerabilidades potenciales que pueden afectar la Sala de Servidores (Activo 2.32)

| Nro. | Nivel | Vulnerabilidades Potenciales |
|---|---|---|
| 1.2.3.1 | 1 | Grado y detalle de la información documentada de la red |
| 1.2.4.1 | 1 | Antecedentes de ataques ocurridos a la red |
| 1.4.1.1 | 2 | Restricción de acceso a personas ajenas al área |
| 1.4.1.2 | 1 | Control personal de limpieza en locales con servidores |
| 1.4.3.1 | 2 | Gestión de fallas dispositivos externos al funcionamiento del equipamiento IT |
| 1.4.4.1 | 1 | Tipo, condiciones e instalación del cableado de red |

## Cuadro 22 (Continuación)

| Nro. | Nivel | Vulnerabilidades Potenciales |
|---|---|---|
| 1.4.4.2 | 1 | Falta de información de otras instalaciones que corran en paralelo |
| 1.4.4.3 | 1 | Actividades que pueden afectar las operaciones |
| 1.4.4.4 | 1 | Actividades externas que pueden afectar las operaciones |
| 1.4.4.5 | 2 | Protecciones antirrayos |
| 1.5.1.1 | 1 | Tipo y regularidad de chequeos |
| 1.5.1.4 | 2 | Documentación y manuales de procedimientos y seguridad |
| 1.5.2.1 | 3 | Administración de emergencias |
| 1.6.1.1 | 2 | Realización y objetos auditados |
| 1.6.1.2 | 1 | Monitoreo y herramientas |
| 1.6.1.3 | 2 | Gestión de logs |
| 1.6.1.4 | 1 | Utilidad auditoria para rastreo de acciones |
| 1.6.1.5 | 1 | Históricos generados |
| 1.7.1.1 | 2 | Existencia, justificaciones |
| 1.7.1.2 | 1 | Alcance del plan |
| 1.7.1.3 | 2 | Responsabilidades y entrenamiento |
| 1.7.1.4 | 2 | Documentación |
| 1.7.2.1 | 3 | Responsabilidades |
| 1.7.2.2 | 2 | Identificación de funciones críticas |
| 1.7.2.3 | 2 | Grupo y responsable |
| 1.7.2.4 | 2 | Inventario de equipamiento |

## Cuadro 23

Amenazas vs. Vulnerabilidades verificadas para la Sala de Servidores (Activo 2.32)

| | Amen. | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 1.7 | 1.8 | 1.9 | 1.10 | 2.1 | 2.2 | 2.4 | 2.10 | 2.11 | 5.4 | 5.5 | 5.29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel / Nivel | 4 | 2 | 4 | 3 | 2 | 2 | 2 | 2 | 2 | 4 | 5 | 3 | 3 | 2 | 3 | 5 | 1 |
| 1.2.3.1 | 1 | | | | | | | | | | X | | | | | | | |
| 1.2.4.1 | 1 | | | | | | | | | | X | | | | | | | |
| 1.4.1.1 | 2 | | | | | | | | | | | | | | | X | | X |
| 1.4.1.2 | 1 | | | | | | | | | | | | | | | | | X |
| 1.4.3.1 | 2 | | | X | | X | | | | | | | | | | | | |
| 1.4.4.1 | 1 | | | | | | | | | | | | | | X | | | |
| 1.4.4.2 | 1 | | | | X | | | | | | | | | | | | | |
| 1.4.4.3 | 1 | | | | | | X | | | | | | | | | | X | X |
| 1.4.4.4 | 1 | | | | | | | X | X | X | | | | | | | X | X |
| 1.4.4.5 | 2 | | X | | | | | | | | | | | | | | | |
| 1.5.1.1 | 1 | | | | | | | | | | | | | X | | | | |
| 1.5.1.4 | 2 | | | | | | | | | | X | | | | | | | |

## Cuadro 23 (Continuación)

| | Amen. | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 1.7 | 1.8 | 1.9 | 1.10 | 2.1 | 2.2 | 2.4 | 2.10 | 2.11 | 5.4 | 5.5 | 5.29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel Nivel | 4 | 2 | 4 | 3 | 2 | 2 | 2 | 2 | 2 | 4 | 5 | 3 | 3 | 2 | 3 | 5 | 1 |
| 1.5.2.1 | 3 | | | | | | | | | | | X | | | | | | |
| 1.6.1.1 | 2 | | | | | | | | | | | | X | | | | | |
| 1.6.1.2 | 1 | | | | | | | | | | | | X | | | | | |
| 1.6.1.3 | 2 | | | | | | | | | | | | X | | | | | |
| 1.6.1.4 | 1 | | | | | | | | | | | | X | | | | | |
| 1.6.1.5 | 1 | | | | | | | | | | | | X | | | | | |
| 1.7.1.1 | 2 | X | | | | | | | | | | | | | | | | |
| 1.7.1.2 | 1 | X | | | | | | | | | | | | | | | | |
| 1.7.1.3 | 2 | X | | | | | | | | | | | | | | | | |
| 1.7.1.4 | 2 | X | | | | | | | | | | | | | | | | |
| 1.7.2.1 | 3 | X | | | | | | | | | | | | | | | | |
| 1.7.2.2 | 2 | X | | | | | | | | | | | | | | | | |
| 1.7.2.3 | 2 | X | | | | | | | | | | | | | | | | |
| 1.7.2.4 | 2 | X | | | | | | | | | | | | | | | | |

## Cuadro 24

Cruce de las Amenazas y las Vulnerabilidades Software y Aplicaciones. Activo 7.1

| Nro. | Niv. | Amenazas Descripción | Vulnerabilidades | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 2.1 | 4 | Falta o insuficiencia de reglas de seguridad en general | 1.7.4.2 | | | | | | | |
| 2.3 | 2 | Recursos incompatibles o inadecuados | 1.6.3.1 | 1.6.3.2 | 1.6.3.3 | | | | | |
| 2.18 | 3 | Procedimientos faltantes o inadecuados para test y liberación de software | 1.3.5.1 | 1.3.5.2 | 1.3.6.1 | 1.3.6.3 | 1.3.7.3 | 1.3.7.6 | | |
| 2.19 | 3 | Documentación faltante o inadecuada | 1.4.5.2 | | | | | | | |
| 2.20 | 2 | Violación de derechos de autor | 1.2.3.3 | 1.3.5.4 | | | | | | |
| 2.21 | 4 | Prueba de software con datos de producción | 1.3.7.7 | | | | | | | |
| 3.3 | 4 | No cumplimiento con las medidas de seguridad IT | 1.1.1.2 | 1.1.1.3 | 1.3.5.4 | 1.7.4.2 | 1.7.4.3 | 1.7.4.4 | 1.7.4.5 | 1.7.4.6 |
| 3.15 | 3 | Errores en la configuración y operación | 1.2.3.3 | 1.2.5.1 | 1.3.6.3 | 1.7.3.1 | 1.7.3.2 | 1.7.3.3 | | |
| 4.4 | 5 | Reconocimiento de vulnerabilidades en el software | 1.3.7.8 | | | | | | | |
| 4.14 | 4 | Vulnerabilidades o errores de software | 1.3.2.1 | 1.3.2.2 | 1.3.3.1 | 1.3.3.2 | 1.3.3.3 | 1.3.3.4 | 1.3.4.1 | 1.3.4.3 |
| | | | 1.3.4.4 | 1.3.5.1 | 1.3.5.2 | 1.3.5.3 | | | | |
| 5.12 | 3 | Caballos de Troya | 1.2.2.3 | | | | | | | |
| 5.13 | 4 | Virus de computador | 1.2.2.1 | 1.2.2.3 | 1.2.2.4 | | | | | |
| 5.18 | 3 | Macro virus | 1.2.2.1 | | | | | | | |

**Cuadro 25**

Vulnerabilidades Potenciales que pueden afectar Software y Aplicaciones. Activo 7.1

| Nro. | Nivel | Descripción |
|---|---|---|
| 1.1.1.2 | 2 | Gestión de bajas de usuarios |
| 1.1.1.3 | 2 | Mantenimiento de cuentas |
| 1.2.2.1 | 3 | No está habilitado para envío y recepción de mail |
| 1.2.2.3 | 2 | No es suficiente la frecuencia de escaneado de las unidades de las computadores |
| 1.2.2.4 | 1 | No se generan discos de rescate en las PCs bajo Win 95/98 |
| 1.2.3.1 | 1 | Grado y detalle de la información documentada de la red |
| 1.2.3.3 | 1 | Documentación de la configuración de las PCs |
| 1.2.5.1 | 3 | Tipo, configuración y nivel de control de firewall |
| 1.3.2.1 | 1 | Existencia de control de cambios para archivos de sistema o bases de datos |
| 1.3.2.2 | 3 | Confidencialidad de datos de laptops y notebooks |
| 1.3.2.3 | 2 | Logs de transacciones y sus detalles |
| 1.3.3.1 | 1 | Existencia de control de cambios para el desarrollo |
| 1.3.3.2 | 1 | Control del contenido de archivos de entrada |
| 1.3.3.3 | 2 | Control de validez de datos ingresados manualmente |
| 1.3.3.4 | 1 | Control de consistencia de datos de salida |
| 1.3.4.1 | 2 | Control de acceso propio de las bases de datos |
| 1.3.4.2 | 1 | Control de instancias de uso |
| 1.3.4.3 | 1 | Chequeo regulares de seguridad |
| 1.3.4.4 | 1 | Marcado o borrado de archivos eliminados |
| 1.3.5.1 | 2 | Controles con que se realiza la instalación y actualización de parches |
| 1.3.5.2 | 1 | Documentación de la instalación o actualización de software |
| 1.3.5.3 | 2 | Control de aplicaciones en máquinas de usuarios |
| 1.3.5.4 | 1 | Control de información que bajan los usuarios de la Web |
| 1.3.6.1 | 1 | Documentación de cambios de emergencia |
| 1.3.6.3 | 1 | Gestión de cambios complejos en archivos de configuración |
| 1.3.6.4 | 2 | Registro de cambios en las configuraciones |
| 1.3.7.3 | 1 | Uso métricas en el desarrollo |
| 1.3.7.6 | 1 | Medidas de seguridad durante las implementaciones |
| 1.3.7.7 | 1 | Forma y documentación de pruebas |
| 1.3.7.8 | 1 | Metodología usada para el mantenimiento |
| 1.4.5.2 | 1 | Inventario de recursos de hardware y software |
| 1.5.1.3 | 1 | Documentación detallada del equipamiento |
| 1.6.3.1 | 1 | Trabajos de mayor uso CPU y memoria |
| 1.6.3.2 | 1 | Datos de mayor tráfico, CPU y memoria |
| 1.6.3.3 | 1 | Aplicaciones de mayor tráfico, CPU y memoria |
| 1.7.3.1 | 1 | Personal de desarrollo |
| 1.7.3.2 | 2 | Técnicos |
| 1.7.3.3 | 2 | Administradores de redes |
| 1.7.4.1 | 3 | Visión y compromiso gerencial superior y medio en la seguridad. |
| 1.7.4.2 | 3 | Reglas de seguridad |
| 1.7.4.3 | 1 | Personal en general - procedimientos |
| 1.7.4.4 | 2 | Personal de desarrollo - procedimientos |
| 1.7.4.5 | 3 | Técnicos - procedimientos |
| 1.7.4.6 | 3 | Administradores de redes - procedimientos |

**Cuadro 26**

Amenazas Vs. Vulnerabilidades verificadas Software y Aplicaciones. Activo 7.1

| | Amen. | 2.1 | 2.3 | 2.18 | 2.19 | 2.20 | 2.21 | 3.3 | 3.15 | 4.4 | 4.14 | 5.12 | 5.13 | 5.18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel / Nivel | 4 | 2 | 3 | 3 | 2 | 4 | 4 | 3 | 5 | 4 | 3 | 4 | 3 |
| 1.1.1.2 | 2 | | | | | | | X | | | | | | |
| 1.1.1.3 | 2 | | | | | | | X | | | | | | |
| 1.2.2.1 | 3 | | | | | | | | | | | | X | X |
| 1.2.2.3 | 2 | | | | | | | | | | | X | X | |
| 1.2.2.4 | 1 | | | | | | | | | | | | X | |
| 1.2.3.1 | 1 | | | | | | | | | | | | | |
| 1.2.3.3 | 1 | | | | | X | | | X | | | | | |
| 1.2.5.1 | 3 | | | | | | | | X | | | | | |
| 1.3.2.1 | 1 | | | | | | | | | | X | | | |
| 1.3.2.2 | 3 | | | | | | | | | | X | | | |
| 1.3.2.3 | 2 | | | | | | | | | | | | | |
| 1.3.3.1 | 1 | | | | | | | | | | X | | | |
| 1.3.3.2 | 1 | | | | | | | | | | X | | | |
| 1.3.3.3 | 2 | | | | | | | | | | X | | | |
| 1.3.3.4 | 1 | | | | | | | | | | X | | | |
| 1.3.4.1 | 2 | | | | | | | | | | X | | | |
| 1.3.4.2 | 1 | | | | | | | | | | | | | |
| 1.3.4.3 | 1 | | | | | | | | | | X | | | |
| 1.3.4.4 | 1 | | | | | | | | | | X | | | |
| 1.3.5.1 | 2 | | | X | | | | | | | X | | | |
| 1.3.5.2 | 1 | | | X | | | | | | | X | | | |
| 1.3.5.3 | 2 | | | | | | | | | | X | | | |
| 1.3.5.4 | 1 | | | | | X | | X | | | | | | |
| 1.3.6.1 | 1 | | | X | | | | | | | | | | |
| 1.3.6.3 | 1 | | | X | | | | | X | | | | | |
| 1.3.6.4 | 2 | | | | | | | | | | | | | |
| 1.3.7.3 | 1 | | | X | | | | | | | | | | |
| 1.3.7.6 | 1 | | | X | | | | | | | | | | |
| 1.3.7.7 | 1 | | | | | | X | | | | | | | |
| 1.3.7.8 | 1 | | | | | | | | | X | | | | |
| 1.4.5.2 | 1 | | | | X | | | | | | | | | |
| 1.5.1.3 | 1 | | | | | | | | | | | | | |
| 1.6.3.1 | 1 | | X | | | | | | | | | | | |
| 1.6.3.2 | 1 | | X | | | | | | | | | | | |
| 1.6.3.3 | 1 | | X | | | | | | | | | | | |
| 1.7.3.1 | 1 | | | | | | | | X | | | | | |
| 1.7.3.2 | 2 | | | | | | | | X | | | | | |
| 1.7.3.3 | 2 | | | | | | | | X | | | | | |

**Cuadro 26 (Continuación)**

| | Amen. | 2.1 | 2.3 | 2.18 | 2.19 | 2.20 | 2.21 | 3.3 | 3.15 | 4.4 | 4.14 | 5.12 | 5.13 | 5.18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vulner.** | **Nivel Nivel** | **4** | **2** | **3** | **3** | **2** | **4** | **4** | **3** | **5** | **4** | **3** | **4** | **3** |
| 1.7.4.1 | 3 | | | | | | | | | | | | | |
| 1.7.4.2 | 3 | X | | | | | | X | | | | | | |
| 1.7.4.3 | 1 | | | | | | | X | | | | | | |
| 1.7.4.4 | 2 | | | | | | | X | | | | | | |
| 1.7.4.5 | 3 | | | | | | | X | | | | | | |
| 1.7.4.6 | 3 | | | | | | | X | | | | | | |

**Cuadro 27**

Cruce de las Amenazas y las vulnerabilidades Servidor Windows S1 (Activo 4.3)

| Amenazas | | | Vulnerabilidades | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Nro.** | **Niv.** | **Descripción** | | | | | | |
| 2.18 | 2 | Reducción de la velocidad de transmisión o ejecución debido a funciones P2P | 1.3.5.4 | | | | | |
| 2.23 | 2 | Planificación inadecuada de los dominios | 1.1.4.3 | | | | | |
| 2.24 | 3 | Protección inadecuada del sistema Windows | 3.1.1 | 3.1.2 | 3.1.3 | 3.1.4 | 3.1.5 | 3.2.1 |
| | | | 3.2.2 | 3.2.3 | 3.3.1 | 3.3.2 | 3.4.1 | 3.4.2 |
| | | | 3.5.1 | 3.5.2 | 3.5.3 | 3.5.4 | 3.6.1 | 3.6.2 |
| | | | 3.6.3 | 3.7.1 | 3.7.2 | 3.8.1 | 3.8.2 | 3.9.1 |
| | | | 3.9.2 | 3.10.1 | 3.10.2 | 3.10.3 | 3.11.1 | 3.12.1 |
| | | | 3.12.2 | 3.12.3 | 3.12.4 | 3.12.5 | 3.14.1 | 3.14.2 |
| | | | 3.15.1 | 3.15.2 | 3.16.1 | 3.16.2 | 3.17.1 | 3.17.2 |
| | | | 3.17.3 | 3.18.1 | 3.18.2 | 3.18.3 | | |
| 4.5 | 4 | Diversidad de posibilidades de acceso a sistemas IT en red | 1.6.2.1 | | | | | |
| 4.16 | 1 | Reconocimiento automático del CD-ROM | 3.12.1 | | | | | |
| 5.13 | 4 | Virus de computador | 1.2.2.1 | 1.2.2.3 | 1.2.2.4 | | | |
| 5.18 | 3 | Macro virus | 1.2.2.1 | 1.2.2.3 | | | | |
| 5.21 | 4 | Mal uso de los derechos de administrador en sistemas Windows NT | 1.6.1.4 | 1.6.1.5 | | | | |
| 5.29 | 3 | Adquisición no autorizada de derechos de administrador con Windows NT | 3.3.1 | 3.17.1 | | | | |

**Cuadro 28**

Vulnerabilidades Potenciales del Servidor Windows S1 (Activo 4.3)

| Nro. | Nivel | Descripción |
|---|---|---|
| 1.1.4.3 | 3 | Mecanismos de control de acceso interno |
| 1.2.2.1 | 3 | No está habilitado para envío y recepción de mail |
| 1.2.2.3 | 2 | No es suficiente la frecuencia de escaneado de las unidades de las computadores |
| 1.2.2.4 | 1 | No se generan discos de rescate |
| 1.3.5.4 | 1 | Control de información que bajan los usuarios de la Web |
| 1.6.1.4 | 1 | Utilidad auditoria para rastreo de acciones |
| 1.6.1.5 | 1 | Históricos generados |
| 1.6.2.1 | 3 | Control de acceso |
| 3.1.1 | 3 | Versión y parches del IIS |
| 3.1.2 | 2 | Versiones 4 y 5 del IIS; ACL y directorios |
| 3.1.3 | 2 | Habilitación del log del IIS |
| 3.1.4 | 3 | WebDav ntdll.dll en IIS 5.0 |
| 3.1.5 | 2 | Aplicaciones de muestra en directorios iissamples, iishelp y msadc |
| 3.2.1 | 3 | Versión y parches del SQL Server |
| 3.2.2 | 2 | Log autenticación servidor SQL |
| 3.2.3 | 2 | Cuenta SA, contraseña |
| 3.3.1 | 3 | Autenticación, algoritmo usado |
| 3.3.2 | 3 | Archivo hashes LM, habilitación autenticación a través de la red |
| 3.4.1 | 3 | Versión y parches del Internet Explorer |
| 3.4.2 | 2 | Nivel seguridad del IE |
| 3.5.1 | 3 | Uso SMB, conectividad NetBios |
| 3.5.2 | 2 | Sesión nula, registro anónimo |
| 3.5.3 | 3 | Acceso remoto al registry |
| 3.5.4 | 3 | rpc y parches |
| 3.6.1 | 3 | Versión y parches del MDAC |
| 3.6.2 | 2 | Archivo msadcs.dll con NT 4.0 e IIS 3.0 o 4.0 |
| 3.6.3 | 1 | Versión y SP del Jet Engine |
| 3.7.1 | 3 | Habilitación del Windows Scripting Host |
| 3.7.2 | 1 | Forma de ejecución de scripts |
| 3.8.1 | 2 | Ventana de vista previa del Outlook/Outlook Express |
| 3.8.2 | 1 | Restricción zona de seguridad del Outlook Express |
| 3.9.1. | 3 | Puertos de aplicaciones P2P |
| 3.9.2 | 2 | Existencia en disco de archivos propios de P2P |
| 3.10.1 | 2 | Versión y puertos habilitados del SNMP |
| 3.10.2 | 3 | Nombres comunidad por default del SNMP |
| 3.10.3 | 2 | Chequeo registros MIB del SNMP |
| 3.11.1 | 3 | Registros bajo SecurePipeServers |
| 3.12.1 | 3 | Registro Winlogon |
| 3.12.2 | 2 | Registro LanMan Print Services, para no poder agregar drivers impresión |
| 3.12.3 | 2 | Registro Subsystems, OS/2 y Posix |
| 3.12.4 | 2 | Registro bajo EventLog, para que no se vean los logs de aplicaciones y sistema |
| 3.12.5 | 2 | Registro Session Manager, atributos recursos compartidos, borrado archivo páginas |
| 3.14.1 | 2 | Uso del passfilt.dll |
| 3.14.2 | 1 | Uso del syskey.exe |

## Cuadro 28 (Continuación)

| Nro. | Nivel | Descripción |
|---|---|---|
| 3.15.1 | 3 | Se usa FAT |
| 3.15.2 | 2 | Grupos Everyone (Todos) y/o Usuarios controlados |
| 3.16.1 | 2 | Logs en Event Viewer |
| 3.16.2 | 1 | Nombres existentes en registro HKLM\System\CurentControlSet\Control\Lsa |
| 3.17.1 | 2 | Existencia y/o restricciones de acceso de archivos ejecutables de cuidado |
| 3.17.2 | 1 | Ubicación de los archivos ejecutables de cuidado |
| 3.17.3 | 2 | Existencia del programa rollback.exe |
| 3.18.1 | 2 | Existencia de c:\winnt\system32\os2 y subdirectorios |
| 3.18.2 | 2 | Archivos del os2 y posix en c:\winnt\system32 |
| 3.18.3 | 1 | Registros os2 subsystem for nt |

## Cuadro 29

Amenazas vs. Vulnerabilidades verificadas Servidor Windows S1 (Activo 4.3)

| | Amen. | 2.18 | 2.23 | 2.24 | 4.5 | 4.16 | 5.13 | 5.18 | 5.21 | 5.29 |
|---|---|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel / Nivel | 2 | 2 | 3 | 4 | 1 | 4 | 3 | 4 | 3 |
| 1.1.4.3 | 3 | | X | | | | | | | |
| 1.2.2.1 | 3 | | | | | | X | X | | |
| 1.2.2.3 | 2 | | | | | | X | X | | |
| 1.2.2.4 | 1 | | | | | | X | | | |
| 1.3.5.4 | 1 | X | | | | | | | | |
| 1.6.1.4 | 1 | | | | | | | | X | |
| 1.6.1.5 | 1 | | | | | | | | X | |
| 1.6.2.1 | 3 | | | | X | | | | | |
| 3.1.1 | 3 | | | X | | | | | | |
| 3.1.2 | 2 | | | X | | | | | | |
| 3.1.3 | 2 | | | X | | | | | | |
| 3.1.4 | 3 | | | X | | | | | | |
| 3.1.5 | 2 | | | X | | | | | | |
| 3.2.1 | 3 | | | X | | | | | | |
| 3.2.2 | 2 | | | X | | | | | | |
| 3.2.3 | 2 | | | X | | | | | | |
| 3.3.1 | 3 | | | X | | | | | | X |
| 3.3.2 | 3 | | | X | | | | | | |
| 3.4.1 | 3 | | | X | | | | | | |
| 3.4.2 | 2 | | | X | | | | | | |
| 3.5.1 | 3 | | | X | | | | | | |
| 3.5.2 | 2 | | | X | | | | | | |
| 3.5.3 | 3 | | | X | | | | | | |
| 3.5.4 | 3 | | | X | | | | | | |
| 3.6.1 | 3 | | | X | | | | | | |
| 3.6.2 | 2 | | | X | | | | | | |
| 3.6.3 | 1 | | | X | | | | | | |

## Cuadro 29

| | Amen. | 2.18 | 2.23 | 2.24 | 4.5 | 4.16 | 5.13 | 5.18 | 5.21 | 5.29 |
|---|---|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel Nivel | 2 | 2 | 3 | 4 | 1 | 4 | 3 | 4 | 3 |
| 3.7.1 | 3 | | | X | | | | | | |
| 3.7.2 | 1 | | | X | | | | | | |
| 3.8.1 | 2 | | | X | | | | | | |
| 3.8.2 | 1 | | | X | | | | | | |
| 3.9.1. | 3 | | | X | | | | | | |
| 3.9.2 | 2 | | | X | | | | | | |
| 3.10.1 | 2 | | | X | | | | | | |
| 3.10.2 | 3 | | | X | | | | | | |
| 3.10.3 | 2 | | | X | | | | | | |
| 3.11.1 | 3 | | | X | | | | | | |
| 3.12.1 | 3 | | | X | | X | | | | |
| 3.12.2 | 2 | | | X | | | | | | |
| 3.12.3 | 2 | | | X | | | | | | |
| 3.12.4 | 2 | | | X | | | | | | |
| 3.12.5 | 2 | | | X | | | | | | |
| 3.14.1 | 2 | | | X | | | | | | |
| 3.14.2 | 1 | | | X | | | | | | |
| 3.15.1 | 3 | | | X | | | | | | |
| 3.15.2 | 2 | | | X | | | | | | |
| 3.16.1 | 2 | | | X | | | | | | |
| 3.16.2 | 1 | | | X | | | | | | |
| 3.17.1 | 2 | | | X | | | | | | X |
| 3.17.2 | 1 | | | X | | | | | | |
| 3.17.3 | 2 | | | X | | | | | | |
| 3.18.1 | 2 | | | X | | | | | | |
| 3.18.2 | 2 | | | X | | | | | | |
| 3.18.3 | 1 | | | X | | | | | | |

## Cuadro 30

Cruce de las Amenazas y las vulnerabilidades Servidor Windows S4 (Activo 4.3)

| Amenazas | | | Vulnerabilidades | | | | | |
|---|---|---|---|---|---|---|---|---|
| Nro. | Niv. | Descripción | | | | | | |
| 2.18 | 2 | Reducción de la velocidad de transmisión o ejecución debido a funciones P2P | 1.3.5.4 | | | | | |
| 2.23 | 2 | Planificación inadecuada de los dominios | | | | | | |
| 2.24 | 3 | Protección inadecuada del sistema Windows | 3.1.1 | 3.1.2 | 3.1.3 | 3.1.4 | 3.1.5 | 3.3.1 |
| | | | 3.3.2 | 3.4.1 | 3.4.2 | 3.6.1 | 3.6.2 | 3.7.1 |
| | | | 3.7.2 | 3.8.2 | 3.10.1 | 3.10.2 | 3.12.1 | 3.12.3 |
| | | | 3.12.4 | 3.12.5 | 3.14.1 | 3.14.2 | 3.15.2 | 3.16.1 |
| | | | 3.16.2 | 3.18.1 | 3.18.2 | 3.18.3 | | |

**Cuadro 30 (Continuación)**

| Amenazas | | | Vulnerabilidades |
|---|---|---|---|
| **Nro.** | **Niv.** | **Descripción** | |
| 4.5 | 4 | Diversidad de posibilidades de acceso a sistemas IT en red | |
| 4.16 | 1 | Reconocimiento automático del CD-ROM | 3.12.1 |
| 5.13 | 4 | Virus de computador | 1.2.2.1 |
| 5.18 | 3 | Macrovirus | 1.2.2.1 |
| 5.21 | 4 | Mal uso de los derechos de administrador en sistemas Windows NT | 1.6.1.4 1.6.1.5 |
| 5.29 | 3 | Adquisición no autorizada de derechos de administrador con Windows NT | 3.3.1 |

**Cuadro 31**

Vulnerabilidades Potenciales del Servidor Windows S4 (Activo 4.3)

| Nro. | Nivel | Descripción |
|---|---|---|
| 1.1.4.3 | 3 | Mecanismos de control de acceso interno |
| 1.2.2.1 | 3 | No está habilitado para envío y recepción de mail |
| 1.2.2.3 | 2 | No es suficiente la frecuencia de escaneado de las unidades de las computadores |
| 1.2.2.4 | 1 | No se generan discos de rescate |
| 1.3.5.4 | 1 | Control de información que bajan los usuarios de la Web |
| 1.6.1.4 | 1 | Utilidad auditoría para rastreo de acciones |
| 1.6.1.5 | 1 | Históricos generados |
| 1.6.2.1 | 3 | Control de acceso |
| 3.1.1 | 3 | Versión y parches del IIS |
| 3.1.2 | 2 | Versiones 4 y 5 del IIS; ACL y directorios |
| 3.1.3 | 2 | Habilitación del log del IIS |
| 3.1.4 | 3 | WebDav ntdll.dll en IIS 5.0 |
| 3.1.5 | 2 | Aplicaciones de muestra en directorios iissamples, iishelp y msadc |
| 3.2.1 | 3 | Versión y parches del SQL Server |
| 3.2.2 | 2 | Log autenticación servidor SQL |
| 3.2.3 | 2 | Cuenta SA, contraseña |
| 3.3.1 | 3 | Autenticación, algoritmo usado |
| 3.3.2 | 3 | Archivo hashes LM, habilitación autenticación a través de la red |
| 3.4.1 | 3 | Versión y parches del Internet Explorer |
| 3.4.2 | 2 | Nivel seguridad del IE |
| 3.5.1 | 3 | Uso SMB, conectividad NetBios |
| 3.5.2 | 2 | Sesión nula, registro anónimo |
| 3.5.3 | 3 | Acceso remoto al registry |
| 3.5.4 | 3 | rpc y parches |
| 3.6.1 | 3 | Versión y parches del MDAC |
| 3.6.2 | 2 | Archivo msadcs.dll con NT 4.0 e IIS 3.0 o 4.0 |
| 3.6.3 | 1 | Versión y SP del Jet Engine |
| 3.7.1 | 3 | Habilitación del Windows Scripting Host |
| 3.7.2 | 1 | Forma de ejecución de scripts |

## Cuadro 31 (Continuación)

| Nro. | Nivel | Descripción |
|---|---|---|
| 3.8.1 | 2 | Ventana de vista previa del Outlook/Outlook Express |
| 3.8.2 | 1 | Restricción zona de seguridad del Outlook Express |
| 3.9.1 | 3 | Puertos de aplicaciones P2P |
| 3.9.2 | 2 | Existencia en disco de archivos propios de P2P |
| 3.10.1 | 2 | Versión y puertos habilitados del SNMP |
| 3.10.2 | 3 | Nombres comunidad por default del SNMP |
| 3.10.3 | 2 | Chequeo registros MIB del SNMP |
| 3.11.1 | 3 | Registros bajo SecurePipeServers |
| 3.12.1 | 3 | Registro Winlogon |
| 3.12.2 | 2 | Registro LanMan Print Services, para no poder agregar drivers impresión |
| 3.12.3 | 2 | Registro Subsystems, OS/2 y Posix |
| 3.12.4 | 2 | Registro bajo EventLog, para que no se vean los logs de aplicaciones y sistema |
| 3.12.5 | 2 | Registro Session Manager, atributos recursos compartidos, borrado archivo páginas |
| 3.14.1 | 2 | Uso del passfilt.dll |
| 3.14.2 | 1 | Uso del syskey.exe |
| 3.15.1 | 3 | Se usa FAT |
| 3.15.2 | 2 | Grupos Everyone (Todos) y/o Usuarios controlados |
| 3.16.1 | 2 | Logs en Event Viewer |
| 3.16.2 | 1 | Nombres existentes en registro HKLM\System\CurentControlSet\Control\Lsa |
| 3.17.1 | 2 | Existencia y/o restricciones de acceso de archivos ejecutables de cuidado |
| 3.17.2 | 1 | Ubicación de los archivos ejecutables de cuidado |
| 3.17.3 | 2 | Existencia del programa rollback.exe |
| 3.18.1 | 2 | Existencia de c:\winnt\system32\os2 y subdirectorios |
| 3.18.2 | 2 | Archivos del os2 y posix en c:\winnt\system32 |
| 3.18.3 | 1 | Registros os2 subsystem for nt |

## Cuadro 32

Amenazas vs. Vulnerabilidades verificadas Servidor Windows S4 (Activo 4.3)

| | Amen. | 2.18 | 2.24 | 4.16 | 5.13 | 5.18 | 5.21 | 5.29 |
|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel / Nivel | 2 | 3 | 1 | 4 | 3 | 4 | 3 |
| 1.1.4.3 | 3 | | | | | | | |
| 1.2.2.1 | 3 | | | | | | | |
| 1.2.2.3 | 2 | | | | | | | |
| 1.2.2.4 | 1 | | | | X | X | | |
| 1.3.5.4 | 1 | X | | | | | | |
| 1.6.1.4 | 1 | | | | | | X | |
| 1.6.1.5 | 1 | | | | | | X | |
| 1.6.2.1 | 3 | | | | | | | |
| 3.1.1 | 3 | | X | | | | | |
| 3.1.2 | 2 | | X | | | | | |
| 3.1.3 | 2 | | X | | | | | |

**Cuadro 32 (Continuación)**

| | Amen. | 2.18 | 2.24 | 4.16 | 5.13 | 5.18 | 5.21 | 5.29 |
|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel Nivel | 2 | 3 | 1 | 4 | 3 | 4 | 3 |
| 3.1.4 | 3 | | X | | | | | |
| 3.1.5 | 2 | | X | | | | | |
| 3.2.1 | 3 | | | | | | | |
| 3.2.2 | 2 | | | | | | | |
| 3.2.3 | 2 | | | | | | | |
| 3.3.1 | 3 | | X | | | | | X |
| 3.3.2 | 3 | | X | | | | | |
| 3.4.1 | 3 | | X | | | | | |
| 3.4.2 | 2 | | X | | | | | |
| 3.5.1 | 3 | | | | | | | |
| 3.5.2 | 2 | | | | | | | |
| 3.5.3 | 3 | | | | | | | |
| 3.5.4 | 3 | | | | | | | |
| 3.6.1 | 3 | | | | | | | |
| 3.6.2 | 2 | | X | | | | | |
| 3.6.3 | 1 | | | | | | | |
| 3.7.1 | 3 | | X | | | | | |
| 3.7.2 | 1 | | X | | | | | |
| 3.8.1 | 2 | | | | | | | |
| 3.8.2 | 1 | | X | | | | | |
| 3.9.1 | 3 | | | | | | | |
| 3.9.2 | 2 | | | | | | | |
| 3.10.1 | 2 | | X | | | | | |
| 3.10.2 | 3 | | X | | | | | |
| 3.10.3 | 2 | | | | | | | |
| 3.11.1 | 3 | | | | | | | |
| 3.12.1 | 3 | | X | X | | | | |
| 3.12.2 | 2 | | | | | | | |
| 3.12.3 | 2 | | X | | | | | |
| 3.12.4 | 2 | | X | | | | | |
| 3.12.5 | 2 | | X | | | | | |
| 3.14.1 | 2 | | X | | | | | |
| 3.14.2 | 1 | | X | | | | | |
| 3.15.1 | 3 | | | | | | | |
| 3.15.2 | 2 | | X | | | | | |
| 3.16.1 | 2 | | X | | | | | |
| 3.16.2 | 1 | | X | | | | | |
| 3.17.1 | 2 | | | | | | | |
| 3.17.2 | 1 | | | | | | | |
| 3.17.3 | 2 | | | | | | | |
| 3.18.1 | 2 | | X | | | | | |
| 3.18.2 | 2 | | X | | | | | |
| 3.18.3 | 1 | | X | | | | | |

## Cuadro 33

Cruce de las Amenazas y las vulnerabilidades Firewall (Activo 5.3)

| Amenazas | | | Vulnerabilidades | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Nro.** | **Niv.** | **Descripción** | | | | | | |
| 2.17 | 4 | Pérdida de confidencialidad de datos sensibles de la red a proteger | 2.1.1 | 2.2.2 | 2.2.3 | 2.3.3 | 2.5.1 | 2.6.1 |
| | | | 2.6.2 | 2.6.3 | 2.8.2 | 2.8.3 | 2.8.5 | 2.8.6 |
| | | | 2.8.9 | 2.8.10 | 2.9.1 | 2.9.3 | 2.9.4 | 2.10.1 |
| | | | 2.10.4 | 2.11.2 | 2.11.3 | 2.11.4 | 2.11.6 | 2.11.7 |
| | | | 2.11.8 | 2.11.9 | 2.11.11 | 2.11.12 | 2.11.14 | 2.11.15 |
| | | | 2.12.1 | 2.12.2 | 2.14.1 | | | |
| 3.10 | 4 | Exportación incorrecta de sistemas de archivos bajo Linux | 2.1.1 | 2.4.2 | 2.6.4 | 2.13.1 | | |
| 3.11 | 4 | Configuración impropia del sendmail | 1.4.3.1 | 2.7.1 | 2.8.11 | 2.11.5 | | |
| 4.1 | 2 | Disrupciones en la fuente de energía | 1.4.3.1 | 2.4.1 | 2.8.7 | 2.11.10 | | |
| 4.13 | 4 | Autenticación faltante o de pobre calidad | 2.2.1 | 2.4.3 | 2.8.8 | | | |
| 5.30 | 1 | Sabotaje | 1.4.3.1 | 2.9.4 | | | | |

## Cuadro 34

Vulnerabilidades Potenciales del Firewall (Activo 5.3)

| Nro. | Nivel | Descripción |
|---|---|---|
| 1.4.3.1 | 2 | Gestión de fallas dispositivos externos al funcionamiento del equipamiento IT |
| 2.1.1 | 2 | Servicios habilitados innecesarios |
| 2.2.1 | 2 | Instalación/ISC, versión y parches Bind |
| 2.2.2 | 2 | Actualización dinámica del DNS |
| 2.2.3 | 2 | Demonio named habilitado en servidores no DNS |
| 2.3.1 | 3 | RPC habilitado |
| 2.3.3 | 2 | Servicios RPC que se pueden explotar |
| 2.4.1 | 2 | Versión SNMP y puertos habilitados |
| 2.4.2 | 3 | Nombres comunidad SNMP por default |
| 2.4.3 | 2 | Chequeo registros MIB del SNMP |
| 2.5.1 | 1 | Instalación y versión ssh |
| 2.6.1 | 3 | Versión NIS |
| 2.6.2 | 3 | Ubicación password del root con NIS |
| 2.6.3 | 2 | Versión NFS |
| 2.6.4 | 3 | Configuración archivo export y montaje de sistema de archivos NFS |
| 2.7.1 | 1 | Versión Open SSL |
| 2.8.1 | 3 | Habilitación y funcionalidad anónima ftp |
| 2.8.2 | 3 | Sin uso de password en el modo de subida ftp |
| 2.8.3 | 3 | No hay restricciones y mecanismos para direcciones IP o dominios en ftp |
| 2.8.5 | 3 | Especificación de las cuentas administrativas en archivo ftpusers |
| 2.8.6 | 3 | No hay diferenciación archivos contraseñas ftp con los del OS |
| 2.8.7 | 2 | Permisos y propietarios del raíz y subdirectorios etc y bin del ftp anónimo |
| 2.8.8 | 2 | Permisos y propietarios de archivos de subdirectorios etc y bin |
| 2.8.9 | 2 | Permisos y propietarios directorio home ~ftp/ |
| 2.8.10 | 3 | Existencia de archivos .rhosts y .forward |

## Cuadro 34 (Continuación)

| Nro. | Nivel | Descripción |
|---|---|---|
| 2.8.11 | 3 | Restricciones de escritura para everyone en directorios ftp y sus archivos |
| 2.9.1 | 2 | Hay cuentas extras con UID 0, o sin contraseñas en el archivo passwd |
| 2.9.2 | 3 | tftp habilitado |
| 2.9.3 | 3 | tftp necesario pero sin precauciones de acceso restringido |
| 2.9.4 | 2 | No se usa un programa para mejorar la elección de contraseñas |
| 2.10.1 | 2 | Permisos y propietarios no adecuados en archivos de servicios de red |
| 2.10.2 | 2 | Cron acepta usuarios ordinarios |
| 2.10.3 | 3 | Se puede registrar como root en la consola en forma remota |
| 2.10.4 | 3 | Terminales no adecuados en el archivo de terminal seguro |
| 2.11.1 | 2 | Archivos .exrc no justificados |
| 2.11.2 | 2 | Archivos .forward en directorios home de usuarios |
| 2.11.3 | 2 | Umask inadecuado de algunos programas |
| 2.11.4 | 2 | Restricciones de acceso no adecuadas en algunos archivos bajo /etc |
| 2.11.5 | 3 | Escritura indebida de los archivos log |
| 2.11.6 | 2 | Características extendidas (inmutabilidad y sólo anexado) no habilitadas |
| 2.11.7 | 2 | Inadecuados permisos, propiedad y grupo de /vmunix |
| 2.11.8 | 3 | Archivos que no debieran ser propiedad sino de root, y /tmp que no tiene el sticky-bit |
| 2.11.9 | 3 | Archivos o directorios no esperados que son escribibles por cualquiera |
| 2.11.10 | 2 | Archivos que no debieran tener seteados el bit SUID o SGID |
| 2.11.11 | 2 | Umask inadecuado de algunos usuarios |
| 2.11.12 | 2 | Archivos ordinarios en el directorio /dev |
| 2.11.13 | 2 | Archivos especiales fuera de /dev |
| 2.11.14 | 2 | Archivos ejecutables y sus directorios ascendentes escribibles por grupos o cualquiera |
| 2.11.15 | 2 | Archivos sin propietarios |
| 2.12.1 | 3 | No se han definido los archivos log adecuados para seguridad |
| 2.12.2 | 2 | No se usan las extensiones de seguridad de Linux para los archivos log |
| 2.13.1 | 2 | Inadecuados permisos y propiedad del archivo /etc/export |
| 2.14.1 | 3 | Parches y actualizaciones Linux |

## Cuadro 35

Amenazas vs. Vulnerabilidades verificadas Firewall (Activo 5.3)

| | Amen. | 2.17 | 3.10 | 3.11 | 4.1 | 4.13 | 5.30 |
|---|---|---|---|---|---|---|---|
| Vulner. | Nivel Nivel | 4 | 4 | 4 | 2 | 4 | 1 |
| 1.4.3.1 | 2 | | | X | X | | X |
| 2.1.1 | 2 | X | X | | | | |
| 2.2.1 | 2 | | | | | X | |
| 2.2.2 | 2 | X | | | | | |
| 2.2.3 | 2 | X | | | | | |
| 2.3.1 | 3 | | | | | | |
| 2.3.3 | 2 | X | | | | | |
| 2.4.1 | 2 | | | | X | | |
| 2.4.2 | 3 | | X | | | | |

**Cuadro 35 (Continuación)**

| | Amen. | 2.17 | 3.10 | 3.11 | 4.1 | 4.13 | 5.30 |
|---|---|---|---|---|---|---|---|
| **Vulner.** | **Nivel Nivel** | **4** | **4** | **4** | **2** | **4** | **1** |
| 2.4.3 | 2 | | | | | X | |
| 2.5.1 | 1 | X | | | | | |
| 2.6.1 | 3 | X | | | | | |
| 2.6.2 | 3 | X | | | | | |
| 2.6.3 | 2 | X | | | | | |
| 2.6.4 | 3 | | X | | | | |
| 2.7.1 | 1 | | | X | | | |
| 2.8.1 | 3 | | | | | | |
| 2.8.2 | 3 | X | | | | | |
| 2.8.3 | 3 | X | | | | | |
| 2.8.5 | 3 | X | | | | | |
| 2.8.6 | 3 | X | | | | | |
| 2.8.7 | 2 | | | | X | | |
| 2.8.8 | 2 | | | | | X | |
| 2.8.9 | 2 | X | | | | | |
| 2.8.10 | 3 | X | | | | | |
| 2.8.11 | 3 | | | X | | | |
| 2.9.1 | 2 | X | | | | | |
| 2.9.2 | 3 | | | | | | |
| 2.9.3 | 3 | X | | | | | |
| 2.9.4 | 2 | X | | | | | X |
| 2.10.1 | 2 | X | | | | | |
| 2.10.2 | 2 | X | | | | | |
| 2.10.3 | 3 | X | | | | | |
| 2.10.4 | 3 | X | | | | | |
| 2.11.1 | 2 | | | | | | |
| 2.11.2 | 2 | X | | | | | |
| 2.11.3 | 2 | X | | | | | |
| 2.11.4 | 2 | X | | | | | |
| 2.11.5 | 3 | | | X | | | |
| 2.11.6 | 2 | X | | | | | |
| 2.11.7 | 2 | X | | | | | |
| 2.11.8 | 3 | X | | | | | |
| 2.11.9 | 3 | X | | | | | |
| 2.11.10 | 2 | | | | X | | |
| 2.11.11 | 2 | X | | | | | |
| 2.11.12 | 2 | X | | | | | |
| 2.11.13 | 2 | | | | | | |
| 2.11.14 | 2 | X | | | | | |
| 2.11.15 | 2 | X | | | | | |
| 2.12.1 | 3 | X | | | | | |
| 2.12.2 | 2 | X | | | | | |
| 2.13.1 | 2 | | X | | | | |
| 2.14.1 | 3 | X | | | | | |

El análisis del riesgo tiene como objetivo identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades. Alberto, (2007), señala que

> "los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del calculo de la posibilidad de que las amenazas y vulnerabilidades relacionadas se junten y causen un incidente". (p. 53)

Para realizar el cálculo del riesgo, se utilizó la metodología de Cramm, a continuación se presenta la matriz de riesgo empleada.

Cuadro 36

Matriz de Riesgo

| **Amenaza** | | **Muy Baja** | | | **Baja** | | | **Media** | | | **Alta** | | | **Muy Alta** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vulnerabilidad** | | **Baja** | **Media** | **Alta** | **Baja** | **Media** | **Alta** | **Baja** | **Media** | **Alta** | **Baja** | **Media** | **Alta** | **Baja** | **Media** | **Alta** |
| **Activo** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 3 |
| | 2 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 |
| | 3 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 |
| | 4 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 |
| | 5 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 |
| | 6 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 |
| | 7 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 |
| | 8 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 7 |
| | 9 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 7 | 7 | 7 | 7 |
| | 10 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 6 | 6 | 7 | 7 | 7 | 7 | 7 |

Nota: Matriz de riesgo según Cramm

| **Riesgos** | |
|---|---|
| **Nivel** | **Valor** |
| Muy Bajo | 1 |
| Bajo | 2 |
| Medio bajo | 3 |
| Medio | 4 |
| Medio alto | 5 |
| Alto | 6 |
| Muy Alto | 7 |

| **Amenazas** | |
|---|---|
| **Nivel** | **Valor** |
| Muy Baja | 1 |
| Baja | 2 |
| Media | 3 |
| Alta | 4 |
| Muy Alta | 5 |

| **Vulnerabilidades** | |
|---|---|
| **Nivel** | **Valor** |
| Baja | 1 |
| Media | 2 |
| Alta | 3 |

A continuación se presenta el cálculo del riesgo para los activos: Sala de Servidores, Aplicaciones y Software, servidores en plataforma Windows y firewall.

**Cuadro 37**

Niveles particulares de riesgo para la Sala de Servidores

| | **Amen.** | **1.2** | **1.3** | **1.4** | **1.5** | **1.6** | **1.7** | **1.8** | **1.9** | **1.10** | **2.1** | **2.2** | **2.4** | **2.10** | **2.11** | **5.4** | **5.5** | **5.29** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vulner.** | **Nivel Nivel** | **4** | **2** | **4** | **3** | **2** | **2** | **2** | **2** | **2** | **4** | **5** | **3** | **3** | **2** | **3** | **5** | **1** |
| 1.2.3.1 | 1 | | | | | | | | | | 6 | | | | | | | |
| 1.2.4.1 | 1 | | | | | | | | | | 6 | | | | | | | |
| 1.4.1.1 | 2 | | | | | | | | | | | | | | | 6 | | 5 |
| 1.4.1.2 | 1 | | | | | | | | | | | | | | | | | 4 |
| 1.4.3.1 | 2 | | | 6 | | 5 | | | | | | | | | | | | |
| 1.4.4.1 | 1 | | | | | | | | | | | | | | 5 | | | |
| 1.4.4.2 | 1 | | | | 5 | | | | | | | | | | | | | |
| 1.4.4.3 | 1 | | | | | | 5 | | | | | | | | | | 7 | 4 |
| 1.4.4.4 | 1 | | | | | | | 5 | 5 | 5 | | | | | | | 7 | 4 |
| 1.4.4.5 | 2 | | 5 | | | | | | | | | | | | | | | |
| 1.5.1.1 | 1 | | | | | | | | | | | | | 5 | | | | |
| 1.5.1.4 | 2 | | | | | | | | | | 6 | | | | | | | |
| 1.5.2.1 | 3 | | | | | | | | | | | 7 | | | | | | |
| 1.6.1.1 | 2 | | | | | | | | | | | | 6 | | | | | |
| 1.6.1.2 | 1 | | | | | | | | | | | | 5 | | | | | |
| 1.6.1.3 | 2 | | | | | | | | | | | | 6 | | | | | |
| 1.6.1.4 | 1 | | | | | | | | | | | | 5 | | | | | |
| 1.6.1.5 | 1 | | | | | | | | | | | | 5 | | | | | |
| 1.7.1.1 | 2 | 6 | | | | | | | | | | | | | | | | |
| 1.7.1.2 | 1 | 6 | | | | | | | | | | | | | | | | |
| 1.7.1.3 | 2 | 6 | | | | | | | | | | | | | | | | |
| 1.7.1.4 | 2 | 6 | | | | | | | | | | | | | | | | |
| 1.7.2.1 | 3 | 7 | | | | | | | | | | | | | | | | |
| 1.7.2.2 | 2 | 6 | | | | | | | | | | | | | | | | |
| 1.7.2.3 | 2 | 6 | | | | | | | | | | | | | | | | |
| 1.7.2.4 | 2 | 6 | | | | | | | | | | | | | | | | |

**Cuadro 38**

Resumen efectos de las amenazas para la Sala de Servidores

| Nro. | Nivel | Descripción | Cantidad Vulnerab. Potenc. | Máximo riesgo |
|---|---|---|---|---|
| 1.2 | 4 | Fallas de los sistemas IT | 8 | 7 |
| 1.3 | 2 | Rayos | 1 | 5 |
| 1.4 | 4 | Incendio | 1 | 6 |
| 1.5 | 3 | Inundación | 1 | 5 |
| 1.6 | 2 | Cables quemados | 1 | 5 |
| 1.7 | 2 | Polvo y suciedad | 1 | 5 |
| 1.8 | 2 | Efectos de catástrofes en el ambiente | 1 | 5 |
| 1.9 | 2 | Problemas causados por grandes eventos públicos | 1 | 5 |
| 1.10 | 2 | Tormentas | 1 | 5 |
| 2.1 | 4 | Falta o insuficiencia de reglas de seguridad en general | 3 | 6 |
| 2.2 | 5 | Conocimiento insuficiente de documentos sobre reglas y procedimientos | 1 | 7 |
| 2.4 | 3 | Monitoreo insuficiente de las medidas de seguridad IT | 5 | 6 |
| 2.10 | 3 | Dimensionamiento insuficiente de redes y centro de cómputo | 1 | 5 |
| 2.11 | 2 | Documentación insuficiente del cableado | 1 | 5 |
| 5.4 | 3 | Robo | 1 | 6 |
| 5.5 | 5 | Vandalismo | 2 | 7 |
| 5.29 | 1 | Sabotaje | 4 | 5 |

En conclusión, la sala de servidores tiene un nivel de riesgo promedio de 5,56 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 34 y los niveles de protección son: para la confidencialidad es medio, para la integridad medio y la disponibilidad es alta.

**Cuadro 39**

Niveles particulares de riesgo Software y Aplicaciones. Activo 7.1

| | Amen. | 2.1 | 2.3 | 2.18 | 2.19 | 2.20 | 2.21 | 3.3 | 3.15 | 4.4 | 4.14 | 5.12 | 5.13 | 5.18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel / Nivel | 4 | 2 | 3 | 3 | 2 | 4 | 4 | 3 | 5 | 4 | 3 | 4 | 3 |
| 1.1.1.2 | 2 | | | | | | | 5 | | | | | | |
| 1.1.1.3 | 2 | | | | | | | 5 | | | | | | |
| 1.2.2.1 | 3 | | | | | | | | | | | | 6 | 5 |
| 1.2.2.3 | 2 | | | | | | | | | | | 5 | 5 | |
| 1.2.2.4 | 1 | | | | | | | | | | | | 5 | |
| 1.2.3.1 | 1 | | | | | | | | | | | | | |

## Cuadro 39 (Continuación)

| | Amen. | 2.1 | 2.3 | 2.18 | 2.19 | 2.20 | 2.21 | 3.3 | 3.15 | 4.4 | 4.14 | 5.12 | 5.13 | 5.18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vulner.** | **Nivel Nivel** | **4** | **2** | **3** | **3** | **2** | **4** | **4** | **3** | **5** | **4** | **3** | **4** | **3** |
| 1.2.3.3 | 1 | | | | | 4 | | | 4 | | | | | |
| 1.2.5.1 | 3 | | | | | | | | 5 | | | | | |
| 1.3.2.1 | 1 | | | | | | | | | | 5 | | | |
| 1.3.2.2 | 3 | | | | | | | | | | 6 | | | |
| 1.3.2.3 | 2 | | | | | | | | | | | | | |
| 1.3.3.1 | 1 | | | | | | | | | | 5 | | | |
| 1.3.3.2 | 1 | | | | | | | | | | 5 | | | |
| 1.3.3.3 | 2 | | | | | | | | | | 5 | | | |
| 1.3.3.4 | 1 | | | | | | | | | | 5 | | | |
| 1.3.4.1 | 2 | | | | | | | | | | 5 | | | |
| 1.3.4.2 | 1 | | | | | | | | | | | | | |
| 1.3.4.3 | 1 | | | | | | | | | | 5 | | | |
| 1.3.4.4 | 1 | | | | | | | | | | 5 | | | |
| 1.3.5.1 | 2 | | | 5 | | | | | | | 5 | | | |
| 1.3.5.2 | 1 | | | 4 | | | | | | | 5 | | | |
| 1.3.5.3 | 2 | | | | | | | | | | 5 | | | |
| 1.3.5.4 | 1 | | | | | 4 | | 5 | | | | | | |
| 1.3.6.1 | 1 | | | 4 | | | | | | | | | | |
| 1.3.6.3 | 1 | | | 4 | | | | | 4 | | | | | |
| 1.3.6.4 | 2 | | | | | | | | | | | | | |
| 1.3.7.3 | 1 | | | 4 | | | | | | | | | | |
| 1.3.7.6 | 1 | | | 4 | | | | | | | | | | |
| 1.3.7.7 | 1 | | | | | | 5 | | | | | | | |
| 1.3.7.8 | 1 | | | | | | | | | 5 | | | | |
| 1.4.5.2 | 1 | | | | 4 | | | | | | | | | |
| 1.5.1.3 | 1 | | | | | | | | | | | | | |
| 1.6.3.1 | 1 | | 4 | | | | | | | | | | | |
| 1.6.3.2 | 1 | | 4 | | | | | | | | | | | |
| 1.6.3.3 | 1 | | 4 | | | | | | | | | | | |
| 1.7.3.1 | 1 | | | | | | | | 4 | | | | | |
| 1.7.3.2 | 2 | | | | | | | | 5 | | | | | |
| 1.7.3.3 | 2 | | | | | | | | 5 | | | | | |
| 1.7.4.1 | 3 | | | | | | | | | | | | | |
| 1.7.4.2 | 3 | 6 | | | | | | 6 | | | | | | |
| 1.7.4.3 | 1 | | | | | | | 5 | | | | | | |
| 1.7.4.4 | 2 | | | | | | | 5 | | | | | | |
| 1.7.4.5 | 3 | | | | | | | 6 | | | | | | |
| 1.7.4.6 | 3 | | | | | | | 6 | | | | | | |

## Cuadro 40

Resumen efectos de las amenazas para Software y Aplicaciones. Activo 7.1

| Nro. | Nivel | Descripción | Cantidad Vulnerab. Potenc. | Máximo riesgo |
|---|---|---|---|---|
| 2.1 | 4 | Falta o insuficiencia de reglas de seguridad en general | 1 | 6 |
| 2.3 | 2 | Recursos incompatibles o inadecuados | 3 | 4 |
| 2.18 | 3 | Procedimientos faltantes o inadecuados para test y liberación de software | 6 | 5 |
| 2.19 | 3 | Documentación faltante o inadecuada | 1 | 4 |
| 2.20 | 2 | Violación de derechos de autor | 2 | 4 |
| 2.21 | 4 | Prueba de software con datos de producción | 1 | 5 |
| 3.3 | 4 | No cumplimiento con las medidas de seguridad IT | 8 | 6 |
| 3.15 | 3 | Errores en la configuración y operación | 6 | 5 |
| 4.4 | 5 | Reconocimiento de vulnerabilidades en el software | 1 | 5 |
| 4.14 | 4 | Vulnerabilidades o errores de software | 12 | 6 |
| 5.12 | 3 | Caballos de Troya | 1 | 5 |
| 5.13 | 4 | Virus de computador | 3 | 6 |
| 5.18 | 3 | Macrovirus | 1 | 5 |

En conclusión, el activo 7.1 Software y Aplicaciones tiene un nivel de riesgo promedio de 4,83 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 46 y los niveles de protección son: para la confidencialidad es medio, para la integridad medio y la disponibilidad es alta.

**Cuadro 41**

Niveles particulares de riesgo Software y Aplicaciones. Activo 7.1

| | Amen. | 2.1 | 2.3 | 2.18 | 2.19 | 2.20 | 2.21 | 3.3 | 3.15 | 4.4 | 4.14 | 5.12 | 5.13 | 5.18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel / Nivel | 4 | 2 | 3 | 3 | 2 | 4 | 4 | 3 | 5 | 4 | 3 | 4 | 3 |
| 1.1.1.2 | 2 | | | | | | | 5 | | | | | | |
| 1.1.1.3 | 2 | | | | | | | 5 | | | | | | |
| 1.2.2.1 | 3 | | | | | | | | | | | | 6 | 5 |
| 1.2.2.3 | 2 | | | | | | | | | | | 5 | 5 | |
| 1.2.2.4 | 1 | | | | | | | | | | | | 5 | |
| 1.2.3.1 | 1 | | | | | | | | | | | | | |
| 1.2.3.3 | 1 | | | | | 4 | | | 4 | | | | | |
| 1.2.5.1 | 3 | | | | | | | | 5 | | | | | |
| 1.3.2.1 | 1 | | | | | | | | | | 5 | | | |
| 1.3.2.2 | 3 | | | | | | | | | | 6 | | | |
| 1.3.2.3 | 2 | | | | | | | | | | | | | |

**Cuadro 41 (Continuación)**

| | Amen. | 2.1 | 2.3 | 2.18 | 2.19 | 2.20 | 2.21 | 3.3 | 3.15 | 4.4 | 4.14 | 5.12 | 5.13 | 5.18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vulner.** | **Nivel Nivel** | **4** | **2** | **3** | **3** | **2** | **4** | **4** | **3** | **5** | **4** | **3** | **4** | **3** |
| 1.3.3.1 | 1 | | | | | | | | | | 5 | | | |
| 1.3.3.2 | 1 | | | | | | | | | | 5 | | | |
| 1.3.3.3 | 2 | | | | | | | | | | 5 | | | |
| 1.3.3.4 | 1 | | | | | | | | | | 5 | | | |
| 1.3.4.1 | 2 | | | | | | | | | | 5 | | | |
| 1.3.4.2 | 1 | | | | | | | | | | | | | |
| 1.3.4.3 | 1 | | | | | | | | | | 5 | | | |
| 1.3.4.4 | 1 | | | | | | | | | | 5 | | | |
| 1.3.5.1 | 2 | | | 5 | | | | | | | 5 | | | |
| 1.3.5.2 | 1 | | | 4 | | | | | | | 5 | | | |
| 1.3.5.3 | 2 | | | | | | | | | | 5 | | | |
| 1.3.5.4 | 1 | | | | | 4 | | 5 | | | | | | |
| 1.3.6.1 | 1 | | | 4 | | | | | | | | | | |
| 1.3.6.3 | 1 | | | 4 | | | | | 4 | | | | | |
| 1.3.6.4 | 2 | | | | | | | | | | | | | |
| 1.3.7.3 | 1 | | | 4 | | | | | | | | | | |
| 1.3.7.6 | 1 | | | 4 | | | | | | | | | | |
| 1.3.7.7 | 1 | | | | | | 5 | | | | | | | |
| 1.3.7.8 | 1 | | | | | | | | | 5 | | | | |
| 1.4.5.2 | 1 | | | | 4 | | | | | | | | | |
| 1.5.1.3 | 1 | | | | | | | | | | | | | |
| 1.6.3.1 | 1 | | 4 | | | | | | | | | | | |
| 1.6.3.2 | 1 | | 4 | | | | | | | | | | | |
| 1.6.3.3 | 1 | | 4 | | | | | | | | | | | |
| 1.7.3.1 | 1 | | | | | | | | 4 | | | | | |
| 1.7.3.2 | 2 | | | | | | | | 5 | | | | | |
| 1.7.3.3 | 2 | | | | | | | | 5 | | | | | |
| 1.7.4.1 | 3 | | | | | | | | | | | | | |
| 1.7.4.2 | 3 | 6 | | | | | | 6 | | | | | | |
| 1.7.4.3 | 1 | | | | | | | 5 | | | | | | |
| 1.7.4.4 | 2 | | | | | | | 5 | | | | | | |
| 1.7.4.5 | 3 | | | | | | | 6 | | | | | | |
| 1.7.4.6 | 3 | | | | | | | 6 | | | | | | |

**Cuadro 42**

Resumen efectos de las amenazas para Software y Aplicaciones. Activo 7.1

| Nro. | Nivel | Descripción | Cantidad Vulnerab. Potenc. | Máximo riesgo |
|---|---|---|---|---|
| 2.1 | 4 | Falta o insuficiencia de reglas de seguridad en general | 1 | 6 |
| 2.3 | 2 | Recursos incompatibles o inadecuados | 3 | 4 |
| 2.18 | 3 | Procedimientos faltantes o inadecuados para test y liberación de software | 6 | 5 |
| 2.19 | 3 | Documentación faltante o inadecuada | 1 | 4 |
| 2.20 | 2 | Violación de derechos de autor | 2 | 4 |
| 2.21 | 4 | Prueba de software con datos de producción | 1 | 5 |
| 3.3 | 4 | No cumplimiento con las medidas de seguridad IT | 8 | 6 |
| 3.15 | 3 | Errores en la configuración y operación | 6 | 5 |
| 4.4 | 5 | Reconocimiento de vulnerabilidades en el software | 1 | 5 |
| 4.14 | 4 | Vulnerabilidades o errores de software | 12 | 6 |
| 5.12 | 3 | Caballos de Troya | 1 | 5 |
| 5.13 | 4 | Virus de computador | 3 | 6 |
| 5.18 | 3 | Macrovirus | 1 | 5 |

En conclusión, el activo 7.1 Software y Aplicaciones tiene un nivel de riesgo promedio de 4,83 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 46 y los niveles de protección son: para la confidencialidad es medio, para la integridad medio y la disponibilidad es alta.

**Cuadro 43**

Niveles particulares de riesgo para el Servidor Windows S1 (Activo 4.3)

| | Amen. | 2.18 | 2.23 | 2.24 | 4.5 | 4.16 | 5.13 | 5.18 | 5.21 | 5.29 |
|---|---|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel / Nivel | 2 | 2 | 3 | 4 | 1 | 4 | 3 | 4 | 3 |
| 1.1.4.3 | 3 | | 6 | | | | | | | |
| 1.2.2.1 | 3 | | | | | | 7 | 6 | | |
| 1.2.2.3 | 2 | | | | | | 7 | 6 | | |
| 1.2.2.4 | 1 | | | | | | 6 | | | |
| 1.3.5.4 | 1 | 5 | | | | | | | | |
| 1.6.1.4 | 1 | | | | | | | | 6 | |
| 1.6.1.5 | 1 | | | | | | | | 6 | |
| 1.6.2.1 | 3 | | | | 7 | | | | | |
| 3.1.1 | 3 | | | 6 | | | | | | |
| 3.1.2 | 2 | | | 6 | | | | | | |

**Cuadro 43 (Continuación)**

| | Amen. | 2.18 | 2.23 | 2.24 | 4.5 | 4.16 | 5.13 | 5.18 | 5.21 | 5.29 |
|---|---|---|---|---|---|---|---|---|---|---|
| **Vulner.** | **Nivel Nivel** | **2** | **2** | **3** | **4** | **1** | **4** | **3** | **4** | **3** |
| 3.1.3 | 2 | | | 6 | | | | | | |
| 3.1.4 | 3 | | | 6 | | | | | | |
| 3.1.5 | 2 | | | 6 | | | | | | |
| 3.2.1 | 3 | | | 6 | | | | | | |
| 3.2.2 | 2 | | | 6 | | | | | | |
| 3.2.3 | 2 | | | 6 | | | | | | |
| 3.3.1 | 3 | | | 6 | | | | | | 6 |
| 3.3.2 | 3 | | | 6 | | | | | | |
| 3.4.1 | 3 | | | 6 | | | | | | |
| 3.4.2 | 2 | | | 6 | | | | | | |
| 3.5.1 | 3 | | | 6 | | | | | | |
| 3.5.2 | 2 | | | 6 | | | | | | |
| 3.5.3 | 3 | | | 6 | | | | | | |
| 3.5.4 | 3 | | | 6 | | | | | | |
| 3.6.1 | 3 | | | 6 | | | | | | |
| 3.6.2 | 2 | | | 6 | | | | | | |
| 3.6.3 | 1 | | | 6 | | | | | | |
| 3.7.1 | 3 | | | 6 | | | | | | |
| 3.7.2 | 1 | | | 6 | | | | | | |
| 3.8.1 | 2 | | | 6 | | | | | | |
| 3.8.2 | 1 | | | 6 | | | | | | |
| 3.9.1. | 3 | | | 6 | | | | | | |
| 3.9.2 | 2 | | | 6 | | | | | | |
| 3.10.1 | 2 | | | 6 | | | | | | |
| 3.10.2 | 3 | | | 6 | | | | | | |
| 3.10.3 | 2 | | | 6 | | | | | | |
| 3.11.1 | 3 | | | 6 | | | | | | |
| 3.12.1 | 3 | | | 6 | | 6 | | | | |
| 3.12.2 | 2 | | | 6 | | | | | | |
| 3.12.3 | 2 | | | 6 | | | | | | |
| 3.12.4 | 2 | | | 6 | | | | | | |
| 3.12.5 | 2 | | | 6 | | | | | | |
| 3.14.1 | 2 | | | 6 | | | | | | |
| 3.14.2 | 1 | | | 6 | | | | | | |
| 3.15.1 | 3 | | | 6 | | | | | | |
| 3.15.2 | 2 | | | 6 | | | | | | |
| 3.16.1 | 2 | | | 6 | | | | | | |
| 3.16.2 | 1 | | | 6 | | | | | | |
| 3.17.1 | 2 | | | 6 | | | | | | 6 |
| 3.17.2 | 1 | | | 6 | | | | | | |
| 3.17.3 | 2 | | | 6 | | | | | | |
| 3.18.1 | 2 | | | 6 | | | | | | |
| 3.18.2 | 2 | | | 6 | | | | | | |
| 3.18.3 | 1 | | | 6 | | | | | | |

**Cuadro 44**

Resumen efectos de las amenazas Servidor Windows S1 (Activo 4.3)

| Nro. | Nivel | Descripción | Cantidad Vulnerab. Potenc. | Máximo riesgo |
|---|---|---|---|---|
| 2.18 | 2 | Reducción de la velocidad de transmisión o ejecución debido a funciones P2P | 1 | 5 |
| 2.23 | 2 | Planificación inadecuada de los dominios | 1 | 6 |
| 2.24 | 3 | Protección inadecuada del sistema Windows NT | 46 | 6 |
| 4.5 | 4 | Diversidad de posibilidades de acceso a sistemas IT en red | 1 | 7 |
| 4.16 | 1 | Reconocimiento automático del CD-ROM | 1 | 6 |
| 5.13 | 4 | Virus de computador | 3 | 7 |
| 5.18 | 3 | Macrovirus | 2 | 6 |
| 5.21 | 4 | Mal uso de los derechos de administrador en sistemas Windows NT | 2 | 6 |
| 5.29 | 3 | Adquisición no autorizada de derechos de administrador con Windows NT | 2 | 6 |

En conclusión, el activo 4.3, servidor Windows S1 tiene un nivel de riesgo promedio de 6,03 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 59 y los niveles de protección son: para la confidencialidad es alto, para la integridad medio y la disponibilidad es alta.

**Cuadro 45**

Niveles particulares de riesgo para el Servidor Windows S4 (Activo 4.3)

| | Amen. | 2.18 | 2.24 | 4.16 | 5.13 | 5.18 | 5.21 | 5.29 |
|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel / Nivel | 2 | 3 | 1 | 4 | 3 | 4 | 3 |
| 1.1.4.3 | 3 | | | | | | | |
| 1.2.2.1 | 3 | | | | | | | |
| 1.2.2.3 | 2 | | | | | | | |
| 1.2.2.4 | 1 | | | | 6 | 6 | | |
| 1.3.5.4 | 1 | 5 | | | | | | |
| 1.6.1.4 | 1 | | | | | | 6 | |
| 1.6.1.5 | 1 | | | | | | 6 | |
| 1.6.2.1 | 3 | | | | | | | |
| 3.1.1 | 3 | | 6 | | | | | |
| 3.1.2 | 2 | | 6 | | | | | |
| 3.1.3 | 2 | | 6 | | | | | |
| 3.1.4 | 3 | | 6 | | | | | |
| 3.1.5 | 2 | | 6 | | | | | |

**Cuadro 45 (Continuación)**

| | Amen. | 2.18 | 2.24 | 4.16 | 5.13 | 5.18 | 5.21 | 5.29 |
|---|---|---|---|---|---|---|---|---|
| Vulner. | Nivel Nivel | 2 | 3 | 1 | 4 | 3 | 4 | 3 |
| 3.2.1 | 3 | | | | | | | |
| 3.2.2 | 2 | | | | | | | |
| 3.2.3 | 2 | | | | | | | |
| 3.3.1 | 3 | | 6 | | | | | 6 |
| 3.3.2 | 3 | | 6 | | | | | |
| 3.4.1 | 3 | | 6 | | | | | |
| 3.4.2 | 2 | | 6 | | | | | |
| 3.5.1 | 3 | | | | | | | |
| 3.5.2 | 2 | | | | | | | |
| 3.5.3 | 3 | | | | | | | |
| 3.5.4 | 3 | | | | | | | |
| 3.6.1 | 3 | | | | | | | |
| 3.6.2 | 2 | | 6 | | | | | |
| 3.6.3 | 1 | | | | | | | |
| 3.7.1 | 3 | | 6 | | | | | |
| 3.7.2 | 1 | | 6 | | | | | |
| 3.8.1 | 2 | | | | | | | |
| 3.8.2 | 1 | | 6 | | | | | |
| 3.9.1 | 3 | | | | | | | |
| 3.9.2 | 2 | | | | | | | |
| 3.10.1 | 2 | | 6 | | | | | |
| 3.10.2 | 3 | | 6 | | | | | |
| 3.10.3 | 2 | | | | | | | |
| 3.11.1 | 3 | | | | | | | |
| 3.12.1 | 3 | | 6 | 6 | | | | |
| 3.12.2 | 2 | | | | | | | |
| 3.12.3 | 2 | | 6 | | | | | |
| 3.12.4 | 2 | | 6 | | | | | |
| 3.12.5 | 2 | | 6 | | | | | |
| 3.14.1 | 2 | | 6 | | | | | |
| 3.14.2 | 1 | | 6 | | | | | |
| 3.15.1 | 3 | | | | | | | |
| 3.15.2 | 2 | | 6 | | | | | |
| 3.16.1 | 2 | | 6 | | | | | |
| 3.16.2 | 1 | | 6 | | | | | |
| 3.17.1 | 2 | | | | | | | |
| 3.17.2 | 1 | | | | | | | |
| 3.17.3 | 2 | | | | | | | |
| 3.18.1 | 2 | | 6 | | | | | |
| 3.18.2 | 2 | | 6 | | | | | |
| 3.18.3 | 1 | | 6 | | | | | |

**Cuadro 46**

Resumen efectos de las amenazas Servidor Windows S4 (Activo 4.3)

| Nro. | Nivel | Descripción | Cantidad Vulnerab. Potenc. | Máximo riesgo |
|---|---|---|---|---|
| 2.18 | 2 | Reducción de la velocidad de transmisión o ejecución debido a funciones P2P | 1 | 5 |
| 2.24 | 3 | Protección inadecuada del sistema Windows NT | 27 | 6 |
| 4.16 | 1 | Reconocimiento automático del CD-ROM | 1 | 6 |
| 5.13 | 4 | Virus de computador | 1 | 6 |
| 5.18 | 3 | Macrovirus | 1 | 6 |
| 5.21 | 4 | Mal uso de los derechos de administrador en sistemas Windows NT | 2 | 6 |
| 5.29 | 3 | Adquisición no autorizada de derechos de administrador con Windows NT | 1 | 6 |

En conclusión, el activo 4.3, servidor Windows S4 tiene un nivel de riesgo promedio de 5,97 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 34 y los niveles de protección son: para la confidencialidad es alto, para la integridad medio y la disponibilidad es alta.

**Cuadro 47**

Niveles particulares de riesgo para el Firewall (Activo 5.3)

| | **Amen.** | **2.17** | **3.10** | **3.11** | **4.1** | **4.13** | **5.30** |
|---|---|---|---|---|---|---|---|
| **Vulner.** | **Nivel / Nivel** | **4** | **4** | **4** | **2** | **4** | **1** |
| 1.4.3.1 | 2 | | | 7 | 6 | | 5 |
| 2.1.1 | 2 | | 7 | | | | |
| 2.2.1 | 2 | | | | | 7 | |
| 2.2.2 | 2 | 7 | | | | | |
| 2.2.3 | 2 | 7 | | | | | |
| 2.3.1 | 3 | | | | | | |
| 2.3.3 | 2 | 7 | | | | | |
| 2.4.1 | 2 | | | | 6 | | |
| 2.4.2 | 3 | | 7 | | | | |
| 2.4.3 | 2 | | | | | 7 | |
| 2.5.1 | 1 | 6 | | | | | |
| 2.6.1 | 3 | 7 | | | | | |
| 2.6.2 | 3 | 7 | | | | | |
| 2.6.3 | 2 | 7 | | | | | |
| 2.6.4 | 3 | | 7 | | | | |
| 2.7.1 | 1 | | | 6 | | | |
| 2.8.1 | 3 | | | | | | |

**Cuadro 47 (Continuación)**

| | Amen. | 2.17 | 3.10 | 3.11 | 4.1 | 4.13 | 5.30 |
|---|---|---|---|---|---|---|---|
| Vulner. | Nivel Nivel | 4 | 4 | 4 | 2 | 4 | 1 |
| 2.8.2 | 3 | 7 | | | | | |
| 2.8.3 | 3 | 7 | | | | | |
| 2.8.5 | 3 | 7 | | | | | |
| 2.8.6 | 3 | 7 | | | | | |
| 2.8.7 | 2 | | | | 6 | | |
| 2.8.8 | 2 | | | | | 7 | |
| 2.8.9 | 2 | 7 | | | | | |
| 2.8.10 | 3 | 7 | | | | | |
| 2.8.11 | 3 | | | 7 | | | |
| 2.9.1 | 2 | 7 | | | | | |
| 2.9.2 | 3 | | | | | | |
| 2.9.3 | 3 | 7 | | | | | |
| 2.9.4 | 2 | 7 | | | | | 5 |
| 2.10.1 | 2 | 7 | | | | | |
| 2.10.2 | 2 | 7 | | | | | |
| 2.10.3 | 3 | 7 | | | | | |
| 2.10.4 | 3 | 7 | | | | | |
| 2.11.1 | 2 | | | | | | |
| 2.11.2 | 2 | 7 | | | | | |
| 2.11.3 | 2 | 7 | | | | | |
| 2.11.4 | 2 | 7 | | | | | |
| 2.11.5 | 3 | | | 7 | | | |
| 2.11.6 | 2 | 7 | | | | | |
| 2.11.7 | 2 | 7 | | | | | |
| 2.11.8 | 3 | 7 | | | | | |
| 2.11.9 | 3 | 7 | | | | | |
| 2.11.10 | 2 | | | | 6 | | |
| 2.11.11 | 2 | 7 | | | | | |
| 2.11.12 | 2 | 7 | | | | | |
| 2.11.13 | 2 | | | | | | |
| 2.11.14 | 2 | 7 | | | | | |
| 2.11.15 | 2 | 7 | | | | | |
| 2.12.1 | 3 | 7 | | | | | |
| 2.12.2 | 2 | 7 | | | | | |
| 2.13.1 | 2 | | 7 | | | | |
| 2.14.1 | 3 | 7 | | | | | |

**Cuadro 48**

Resumen efectos de las amenazas Firewall (Activo 5.3)

| Nro. | Nivel | Descripción | Cantidad Vulnerab. Potenc. | Máximo riesgo |
|---|---|---|---|---|
| 2.17 | 4 | Pérdida de confidencialidad de datos sensibles de la red a proteger | 34 | 7 |
| 3.10 | 4 | Exportación incorrecta de sistemas de archivos bajo Linux | 4 | 7 |
| 3.11 | 4 | Configuración impropia del sendmail | 4 | 7 |
| 4.1 | 2 | Disrupciones en la fuente de energía | 4 | 6 |
| 4.13 | 4 | Autenticación faltante o de pobre calidad | 3 | 7 |
| 5.30 | 1 | Sabotaje | 2 | 5 |

En conclusión, el activo 5.3, Firewall tiene un nivel de riesgo promedio de 6,67 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 52 y los niveles de protección son: para la confidencialidad es medio, para la integridad medio y la disponibilidad es alta.

*Tratamiento del riesgo y el proceso de toma de decisión gerencial*

Una vez efectuados el análisis y la evaluación del riesgo, se debe decidir cuáles acciones se han de tomar con esos activos que están sujetos a riesgos. Los riesgos descubiertos pueden manejarse con una serie de controles para la detección y la prevención, con tácticas para evitar el riesgo o aceptarlo transfiriéndolo a otra organización.

Luego del proceso de identificación de las opciones de tratamiento de riesgo y de haberlas evaluado, la empresa debe decidir cuales objetivos de control y controles escoger para el tratamiento del riesgo y preparar la declaración de aplicabilidad, el cual es un documento muy importante del SGSI, según el ISO 27001:2005, la cláusula 4.2.1 (j) da las exigencias que se deben seguir para estar en conformidad.

*Plan de tratamiento del riesgo*

Una vez que se han tomado las decisiones relacionadas con el tratamiento del riesgo, las actividades para poder implantar estas decisiones tienen que ejecutarse. Para ello se deben identificar y planear las actividades con claridad y distribuir las responsabilidades a las personas, estimar los requerimientos de recursos, el conjunto de entregables, las fechas críticas y la supervisión del progreso.

En esencia, la implantación del plan de tratamiento del riesgo es un proyecto y la universidad debe asignar a la persona idónea para responsabilizarla del proyecto, visualizar los recursos necesarios y manejar los reforzadores de conducta organizacional, que aseguren el correcto desempeño del proyecto.

En el cuadro 49, se muestra una ilustración de un proyecto de desarrollo del plan de tratamiento de riesgo, para el Sistema Administrativo Integrado SAI. Es de destacar, que se deben asignar los recursos y las acciones correspondientes para implementar las decisiones de la gestión del riesgo que deben iniciarse. En la cláusula 4.2.2 (a), el ISO 27001:2005 plantea las exigencias para desarrollar el plan de tratamiento de riesgo.

**Cuadro 49**

Plan de tratamiento del riesgo

| Áreas | Actividades | Control | Activo | Fecha de Culminación | Responsable |
|---|---|---|---|---|---|
| ORTSI | Elaborar procedimientos para el sistema de administración de contraseñas, uso de contraseñas y administración de contraseñas de usuarios. | A.9.2.3<br>A.9.3.1<br>A.9.5.4 | Seguridad y control | 15/01/2008 | Coordinación de Producción y Operaciones |

**Cuadro 49 (Continuación)**

| Áreas | Actividades | Control | Activo | Fecha de Culminación | Responsable |
|---|---|---|---|---|---|
| ORTSI | Elaborar documentos de los procedimientos operativos del SAI | A.10.1.1 | Soporte Servicio de Información | 15/02/2008 | Coordinación de Producción y Operaciones |
| | Realizar controles de cambios cuando ocurra alguna variación en los recursos o en el sistema SAI | A.10.1.2 | Control de cambio | Cada vez que ocurra un cambio | ORTSI |
| | Realizar estadísticas del crecimiento vegetativo del sistema SAI a fin de hacer proyecciones de los requisitos de la capacidad futura del servidor | A.10.3.1 | Soporte Servicio de Información | Mensual | Coordinación de Producción y Operaciones |
| | Instalar antivirus y actualizarlos constantemente para mitigar el riesgo del código malicioso | A.10.4.1 | Mantenimiento e Infraestructura | Semanalmente | Coordinación de Atención a Usuarios |
| | Elaborar un programa de capacitación para la detección y prevención de código malicioso. | A.10.4.1 | Mantenimiento e infraestructura | 15/02/2008 | Coordinación de Atención a Usuarios |

**Cuadro 49 (Continuación)**

| Áreas | Actividades | Control | Activo | Fecha de Culminación | Responsable |
|---|---|---|---|---|---|
| ORTSI | Realizar las copias de seguridad de la información según la política de seguridad acordada. | A.10.5.1 | Soporte Servicio de Información | Semanalmente | Coordinación de Producción y Operaciones |
| | Elaborar un procedimiento para la eliminación segura de los medios de información. (Disco duros, Pendrive, C.D., entre otros) | A.10.7.2 | Mantenimiento e Infraestructura | 15/02/2008 | Coordinación de Atención a Usuarios |
| | Se debe llevar el registro de las actividades del administrador del SAI, así como las de los operadores | A.10.10.4 | Líder Técnico del SAI | Regularmente | Coordinador de Producción y Operaciones |
| | Elaborar registro de las fallas detectada en el sistema y en la infraestructura. | A.10.10.5 | Líder Técnico del SAI | Regularmente | Coordinador de Producción y Operaciones |
| | Elaborar las políticas de control de acceso al sistema SAI | A.11.1.1 | Soporte Ambiente Operativo | 15/02/2008 | Coordinación de Producción y Operaciones |

**Cuadro 49 (Continuación)**

| Áreas | Actividades | Control | Activo | Fecha de Culminación | Responsable |
|---|---|---|---|---|---|
| | Elaborar un procedimiento de registro y des-registro de usuarios para conceder o revocar el acceso al SAI. | A.11.2.1 | Soporte Ambiente Operativo | 15/02/2008 | Coordinador de Producción y Operaciones |
| | Elaborar procedimientos de selección y uso de contraseñas | A.11.3.1 | Soporte Servicio de Información | 30/01/2008 | Coordinador de Producción y Operaciones |
| | Elaborar un procedimiento para el sistema de gestión de contraseñas | A.11.5.3 | Soporte Ambiente Operativo | 30/01/2008 | Coordinador de Producción y Operaciones |
| | Elaborar un plan para la realización de auditorias de sistemas que conlleve a minimizar el riesgo de interrupciones en los procesos administrativos. | A.15.3.1 | Coordinación Nacional de Tecnología e Información | 30/06/2008 | OCTSI |
| | Elaborar un programa detallado de capacitación para el manejo del SAI. | A.8.2.2 | Coordinación Nacional de Tecnología e Información | 30/03/2008 | OCTSI |

**Cuadro 49 (Continuación)**

| Áreas | Actividades | Control | Activo | Fecha de Culminación | Responsable |
|---|---|---|---|---|---|
| ORTSI | Elaborar un documento de la política de seguridad de la información | A.5.1.1 | ORTSI | 30/11/2007 | ORTSI |
| Oficinas donde están los módulos del SAI operativos | Elaborar las políticas de control de accesos a la información o recursos de información del personal externo e interno | A.11.1.1 | Oficina | 15/02/2008 | Oficina |
| | Elaborar una política sobre seguridad de información incluyendo papeles, responsabilidades y sanciones. | A.8.1.1<br>A.8.2.3 | Oficina | 15/02/2008 | Oficina |
| | Elaborar políticas para que los usuarios ejerciten buenas prácticas en la selección y uso de claves. | A.11.3.1<br>A.11.5.3 | Oficina | 15/02/2008 | Oficina |
| | Elaborar un programa detallado de capacitación para crear conciencia sobre la importancia de la seguridad de información y su manejo por el personal de la oficina. | A.8.2.2<br>A.6.1.3 | Oficina | 30/01/2008 | Oficina |

**Cuadro 49 (Continuación)**

| Áreas | Actividades | Control | Activo | Fecha de Culminación | Responsable |
|---|---|---|---|---|---|
| Oficinas donde están los módulos del SAI operativos | Establecer políticas definidas para la asignación de responsabilidades en la protección de activos de información así como de seguridad de información. | A.6.1.3 | Oficina | 15/02/2008 | Oficina |
| | Se debe organizar y mantener actualizada la cadena de contactos (Interno o Externo) con el mayor detalle posible identificando los requisitos de seguridad antes de dar acceso a la información. | A.6.2.2 A.6.2.3 | Oficina | 30/01/2008 | Oficina |

En el anexo J se presentan los procedimientos correspondientes al control A.6.3.1 Reporte de incidente de seguridad, control A.9.2.3 Administración de contraseñas de usuarios, control A. 9.3.1 Uso de contraseñas y control A.9.5.4 Sistema de Administración de contraseñas. Seguidamente, el anexo K presenta un cronograma de cuarenta y cuatro (44) semanas para implementar el SGSI.

*Revisión de los riesgos y la reevaluación*

Los resultados del análisis y la evaluación del riesgo requieren ser revisados con regularidad para visualizar cualquier modificación. Las estructuras organizacionales, las tareas que se ejecutan, la tecnología que se utiliza y las personas en las organizaciones hacen una dinámica que afectan los riesgos valorados en un momento determinado.

En este sentido, la declaración de aplicabilidad, tal como lo exige el ISO 27001:2005 en la cláusula 4.2.1 (4)(j), es un excelente registro de los últimos controles establecidos. Su uso es muy apropiado para mantener un registro de los últimos controles instaurados en el SGSI. En el cuadro 50 se tiene una ilustración de la declaración de aplicabilidad.

**Cuadro 50**

Declaración de aplicabilidad del Sistema Administrativo Integrado

| **Objetivos de control** | **Controles** | **Aplicabilidad** | | **Justificación** |
|---|---|---|---|---|
| | | **SI** | **NO** | |
| A.5.1. Política de Seguridad de la información | A.5.1.1 | X | | Es necesario establecer las políticas de seguridad para los sistemas de información, ya que manejan la información vital de la universidad. Es necesario revisar periódicamente las políticas de seguridad para asegurar que se mantengan adecuadas. |
| | A.5.1.2 | X | | |
| A.6.1 Organización interna | A.6.1.1 | X | | Es necesario tener controles y políticas para el manejo de la seguridad de la información dentro de la universidad. |
| | A.6.1.2 | X | | |
| | A.6.1.3 | X | | |
| | A.6.1.4 | X | | |
| | A.6.1.5 | X | | |
| | A.6.1.6 | X | | |
| | A.6.1.7 | X | | |
| | A.6.1.8 | X | | |

**Cuadro 50 (Continuación)**

| | | | | |
|---|---|---|---|---|
| A.6.2 Partes externas | A.6.2.1 | X | | Se necesita controles para mitigar riesgos con entidades externas. Es necesario establecer requerimientos de seguridad porque hay documentos con información clasificada de la universidad que son trasladados por terceros.} |
| | A.6.2.2 | X | | |
| | A.6.2.3 | X | | |
| A.7.1 Responsabilidad por los activos | A.7.1.1 | X | | Es necesario tener controles y políticas para mantener la protección apropiada de los activos de la universidad. |
| | A.7.1.2 | X | | |
| | A.7.1.3 | X | | |
| A.7.2 Clasificación de la información | A.7.2.1 | X | | Es necesario tener políticas y controles para asegurar que la información reciba un nivel de protección apropiado. |
| | A.7.2.2 | X | | |
| A.8.1 Antes del empleo | A.8.1.1 | X | | Es necesario que los Todos los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO, así como los usuarios de terceras partes comprendan sus responsabilidades, y que sean apropiados para los roles considerados, para mitigar los riesgos de robo, fraude o mal uso de los recursos. |
| | A.8.1.2 | X | | |
| | A.8.1.3 | X | | |
| A.8.2 Durante el empleo | A.8.2.1 | X | | Todos los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO, así como los usuarios de terceras partes deben estar conscientes de las amenazas que tienen los sistemas de información, sus responsabilidades y obligaciones para reducir el riesgo de error humano. |
| | A.8.2.2 | X | | |
| | A.8.2.3 | X | | |

**Cuadro 50 (Continuación)**

| | | | | |
|---|---|---|---|---|
| A.8.3 Terminación o cambio de empleo | A.8.3.1 | X | | Debe asegurarse que los empleados, contratistas y usuarios de terceras partes se retiran de la universidad o son trasladados a otra oficina lo hagan de una manera ordenada. |
| | A.8.3.2 | X | | |
| | A.8.3.3 | X | | |
| A.9.1 Áreas seguras | A.9.1.1 | X | | Es necesario prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones e información de la universidad. |
| | A.9.1.2 | X | | |
| | A.9.1.3 | X | | |
| | A.9.1.4 | X | | |
| | A.9.1.5 | X | | |
| | A.9.1.6 | X | | |
| A.9.2 Seguridad de los equipos | A.9.2.1 | X | | Se debe prevenir las pérdidas, daño o robo de los activos que puedan causar la interrupción de las actividades de la universidad. |
| | A.9.2.2 | X | | |
| | A.9.2.3 | X | | |
| | A.9.2.4 | X | | |
| | A.9.2.5 | X | | |
| | A.9.2.6 | X | | |
| | A.9.2.7 | X | | |
| A.10.1 Procedimiento y responsabilidades de operación | A.10.1.1 | X | | Se debe asegurar la correcta operación de los recursos para el tratamiento de información. |
| | A.10.1.2 | X | | |
| | A.10.1.3 | X | | |
| | A.10.1.4 | X | | |
| A.10.2 Gestión de entrega de servicio de tercera parte | A.10.2.1 | X | | Cuando se realice algún servicio externo se debe implementar controles para mantener el nivel apropiado de seguridad de la información. |
| | A.10.2.2 | X | | |
| | A.10.2.3 | X | | |
| A.10.3 Planificación y aceptación del sistema | A.10.3.1 | X | | Se debe minimizar el riesgo de fallas de los sistemas. |
| | A.10.3.2 | X | | |
| A.10.4 Protección contra código malicioso y movible | A.10.4.1 | X | | Se debe proteger la integridad del software y de la información. No está autorizado el uso de código movible. |
| | A.10.4.2 | | X | |

**Cuadro 50 (Continuación)**

| | | | | |
|---|---|---|---|---|
| A.10.5 Copia de seguridad | A.10.5.1 | X | | Se debe asegurar realizar respaldo del sistema y de las bases de datos. Igualmente se deben probar que las copias de seguridad funcionen correctamente a fin de garantizar la integridad y la disponibilidad de la información. |
| A.10.6 Gestión de seguridad de la red | A.10.6.1 | X | | Se debe proteger la información en la red de datos, así como la infraestructura de soporte. |
| | A.10.6.2 | X | | |
| A.10.7 Manejo de medios de información | A.10.7.1 | X | | Se debe prevenir la divulgación, modificación, eliminación o destrucción no autorizada de los activos e interrupción de las actividades administrativas de la universidad. |
| | A.10.7.2 | X | | |
| | A.10.7.3 | X | | |
| | A.10.7.4 | X | | |
| A.10.8 Intercambio de información | A.10.8.1 | X | | Se debe asegurar el intercambio de información dentro de la universidad y con cualquier entidad externa |
| | A.10.8.2 | X | | |
| | A.10.8.3 | X | | |
| | A.10.8.4 | X | | |
| | A.10.8.5 | X | | |
| A.10.9 Servicio de comercio electrónico | A.10.9.1 | | X | No se realiza comercio electrónico en la universidad. |
| | A.10.9.2 | | X | |
| | A.10.9.3 | | X | |
| A.10.10 Seguimiento | A.10.10.1 | X | | Se debe registrar las actividades de procesamiento de información no autorizada. |
| | A.10.10.2 | X | | |
| | A.10.10.3 | X | | |
| | A.10.10.4 | X | | |
| | A.10.10.5 | X | | |
| | A.10.10.6 | X | | |
| A.11.1 Requisitos del negocio para el control de accesos | A.11.1.1 | X | | Es necesario establecer las políticas de control de acceso. |
| A.11.2 Gestión de acceso de usuarios | A.11.2.1 | X | | Es necesario prevenir el acceso no autorizado a los sistemas de información |
| | A.11.2.2 | X | | |
| | A.11.2.3 | X | | |
| | A.11.2.4 | X | | |

**Cuadro 50 (Continuación)**

| | | | | |
|---|---|---|---|---|
| A.11.3 Responsabilidad de usuarios | A.11.3.1 | X | | Es necesario crear conciencia en los usuarios para que sigan buenas practicas de seguridad a fin de evitar el acceso de usuarios no autorizados y mitigar los riesgos de robo de información o de recursos de procesamiento de información. |
| | A.11.3.2 | X | | |
| | A.11.3.3 | X | | |
| A.11.4 Control de acceso a la red | A.11.4.1 | X | | Es necesario elaborar políticas de acceso para la utilización de los servicios de red. |
| | A.11.4.2 | X | | |
| | A.11.4.3 | X | | |
| | A.11.4.4 | X | | |
| | A.11.4.5 | X | | |
| | A.11.4.6 | | X | |
| | A.11.4.7 | | X | |
| A.11.5 Control de acceso al sistema operativo | A.11.5.1 | | X | Es necesario que todos los usuarios dispongan de un identificador único. Deben existir sistemas para la gestión de contraseñas. |
| | A.11.5.2 | X | | |
| | A.11.5.3 | X | | |
| | A.11.5.4 | X | | |
| | A.11.5.5 | X | | |
| | A.11.5.6 | X | | |
| A.11.6 Control de acceso a las aplicaciones e información | A.11.6.1 | X | | Se debe prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación. |
| | A.11.6.2 | X | | |
| A.11.7 Computación móvil y trabajo a distancia | A.11.7.1 | | X | No se realiza teletrabajo ni recursos de computación móvil. |
| | A.11.7.2 | | X | |
| A.12.1 Requisitos de seguridad de los sistemas de información | A.12.1.1 | X | | Se deben especificar los controles de seguridad para las mejoras del SAI. |
| A.12.2 Procesamiento correcto en las aplicaciones | A.12.2.1 | X | | Se debe prevenir los errores, pérdida, modificación no autorizada o mal uso de la información en el SAI. |
| | A.12.2.2 | X | | |
| | A.12.2.3 | X | | |
| | A.12.2.4 | X | | |
| A.12.3 Controles criptográficos | A.12.3.1 | | X | No se utiliza encriptación de la información, ni gestión de claves. |
| | A.12.3.2 | | X | |

**Cuadro 50 (Continuación)**

| | | | | |
|---|---|---|---|---|
| A.12.4 Seguridad de los archivos del sistema | A.12.4.1 | X | | Se debe asegurar la seguridad de los archivos del sistema. |
| | A.12.4.2 | X | | |
| | A.12.4.3 | X | | |
| A.12.5 Seguridad en los procesos de desarrollo y soporte | A.12.5.1 | X | | Se debe mantener la seguridad del software y la información del sistema SAI. |
| | A.12.5.2 | | X | |
| | A.12.5.3 | X | | |
| | A.12.5.4 | X | | |
| | A.12.5.5 | X | | |
| A.12.6 Gestión de vulnerabilidad técnica | A.12.6.1 | X | | Se deben evaluar las vulnerabilidades del SAI para mitigar el riesgo asociado. |
| A.13.1 Reportar los eventos y debilidades de seguridad de la información | A.13.1.1 | X | | Se deben diseñar formatos para reportar los incidentes de seguridad asociados al SAI para tomar acciones correctivas oportunamente. |
| | A.13.1.2 | X | | |
| A.13.2 Gestión de los incidentes y mejoras de seguridad de la información | A.13.2.1 | X | | Se deben gestionar los incidentes de seguridad de la información. |
| | A.13.2.2 | X | | |
| | A.13.2.3 | X | | |
| A.14.1 Gestión de continuidad del negocio | A.14.1.1 | X | | Se debe diseñar un plan de continuidad del negocio que garantice la reanudación del servicio oportunamente ante la ocurrencia de un evento de seguridad. |
| | A.14.1.2 | X | | |
| | A.14.1.3 | X | | |
| | A.14.1.4 | X | | |
| | A.14.1.5 | X | | |
| A.15.1 Cumplimiento de requisitos legales | A.15.1.1 | X | | Se debe evitar el incumplimiento de cualquier ley, estatuto, obligación reglamentaria y de cualquier requisito de seguridad. |
| | A.15.1.2 | X | | |
| | A.15.1.3 | X | | |
| | A.15.1.4 | X | | |
| | A.15.1.5 | X | | |
| | A.15.1.6 | | X | |
| A.15.2 Cumplimiento con las políticas y normas de seguridad y el cumplimiento técnico | A.15.2.1 | X | | Se debe realizar y evaluar un plan de seguridad de la universidad |
| | A.15.2.2 | X | | |

**Cuadro 50 (Continuación)**

| | | | | |
|---|---|---|---|---|
| A.15.3 Consideraciones de auditoria de los sistemas de información | A.15.3.1 | X | | Elaborar un plan para la realización de auditorias de sistemas que conlleve a minimizar el riesgo de interrupciones de los procesos administrativos de la universidad. |
| | A.15.3.2 | X | | |

# CAPITULO V

# CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

En atención a la metodología empleada para el establecimiento de un Sistema de Gestión de Seguridad de la Información y tomando en consideración los objetivos de la investigación las conclusiones del estudio son las siguientes, las cuales denotan grandes beneficios al implantar el SGSI al sistema de información SAI. En tal sentido, se detalla de acuerdo a las fases ejecutadas en la investigación:

*Fase I. Diagnóstico:* de los resultados obtenidos a través del cuestionario aplicado, así como la observación directa del investigador dieron las siguientes conclusiones:

No existe un documento de política de seguridad de la información

No están establecidos los perímetros de seguridad para las áreas que contienen información crítica de la universidad.

No se cumplen los procedimientos para permitir el acceso sólo al personal autorizado.

El personal tiene escasos conocimientos en el área de seguridad de la información, así como de los estándares aplicados en la materia.

No se aplican procedimientos para proteger los procesos administrativos críticos de la universidad de los efectos de fallas significativas de los sistemas de información y asegurar su reanudación oportuna.

No se lleva una correcta administración y control de la red, es decir, no se implementan todas las medidas posibles para evitar amenazas y mantener la seguridad de los sistemas y aplicaciones que circulan por ella.

No se realizan revisiones periódicas y procedimientos de monitorización del uso de los sistemas.

No existen políticas de control de acceso a la información universitaria.

No existen planes de continuidad del negocio.

Se realizó un instrumento de diagnóstico un "Cuestionario", el cual fue validado y se demostró la confiabilidad, que puede servir como apoyo a futuras investigaciones relacionadas con el tema.

*Fase II. Factibilidad:* Se demostró que existe factibilidad tanto operativa, técnica y económica para establecer un Sistema de Gestión de Seguridad de la Información para el sistema de información del SAI dentro de la UNEXPO Vicerrectorado de Puerto Ordaz.

*Fase III. Establecimiento de un Sistema de Gestión de Seguridad de Información,* se aplicó la cláusula 4.2 de la norma ISO 27001:2005. También se adoptó un método y un enfoque sistemático para el cálculo del riesgo de los activos de información del Sistema Administrativo Integrado.

Al finalizar el establecimiento del SGSI se pueden señalar las siguientes reflexiones:

La esencia de un sistema de gestión de seguridad de la información es mitigar el riesgo al que están sujetos los activos de información, de una determinada empresa.

La correcta identificación de los activos de información, dentro del alcance que tenga el modelo en la empresa, así como todas las interfaces, es fundamental para la adecuada implantación del sistema de gestión de seguridad de la información.

La implementación de un SGSI requiere el despliegue de recursos significativos, por esto las organizaciones deben estar concientes sobre sus razones para implantar el sistema. De allí, que el por qué implementar el SGSI,

debe estar claramente documentado, y debe plantear los costos en contraposición a los beneficios que puedan obtenerse al incrementar la habilidad de gestionar el riesgo de la información en la organización.

El SGSI no puede implantarse de manera aislada, la institución debe considerar los riesgos y las estrategias globales a aplicar. Siempre se debe tener presente que el SGSI es un sistema de gestión, el cual se convierte en una herramienta de la alta gerencia.

La implantación del modelo ISO 27001:2005 requiere una participación completa del nivel estratégico. De allí, que tiene que contemplarse como un proyecto, el cual tiene tiempos asignados a actividades, recursos, responsable que lo controle y lo más importante es que debe contar con el apoyo de la alta gerencia.

La duración en implantar el ISO 27001:2005 dependerá de varios factores, tales como: el alcance del modelo, los recursos disponibles, la participación de la gerencia y la prioridad que se le da al proyecto de implantación. Usualmente es un estimado adecuado calcular unos doce (12) meses.

## Recomendaciones

Las recomendaciones se elaboraron sobre la base de los elementos y acciones que se evidenciaron a través del desarrollo de la investigación, las cuales se detallan a continuación:

En primer lugar, elaborar las Políticas de Seguridad y el Manual de Seguridad de Información que permita organizar y agrupar la documentación considerado por el modelo ISO 27001:2005 como vital, las misma deben ser aprobadas en Consejo Universitario y difundida a toda la comunidad Unexpista.

Evaluar con un asesor reconocido de empresas en Sistemas de Gestión de Seguridad de la Información la propuesta y el plan de tratamiento de riesgo

presentada, para cerciorarse que no se han omitido ningún control y se asegure el éxito en la implantación del SGSI.

Diseñar un “Plan de Formación” en seguridad de la información que se ajuste al SGSI. El mismo debe ser realizado de manera periódica y debe ser tratado como cualquier otra actividad de la universidad, permitiendo que se complementen e integren en todo el SGSI como una parte más, generando concientización y adhesión con el mismo.

Desarrollar un Plan de Gestión de la Continuidad del Negocio (PCN), el mismo lo exige la norma ISO 27001:2005 por medio del control A.14.

Fortalecer el grupo de trabajo Seguridad y Control de la Coordinación de Producción y Operaciones de la ORTSI, con la contratación de un profesional responsable de la gestión de la seguridad de información del Vicerrectorado.

## REFERENCIAS BIBLIOGRAFICAS


Aceituno, V. 2004. *Seguridad de la Información. Expectativas, riesgos y técnicas de protección.* Creaciones Copyright. España.

Alberts, Christopher y Dorofee, Autrey 200). *Managing Information Security Risk*, Nueva York. Addison Wesley

Alexander, A. 2007. *Diseño de un Sistema de Gestión de Seguridad de Información, óptica ISO 27001:2005*. Alfaomega Colombiana S.A. Bogotá, D.C. - Colombia

Amoroso, E. 2004. *Fundamentos de Tecnología de Seguridad Informática*. Prentice Hall.

Ary, W. 1996. *Metodología de la Investigación.* ED.:Ediciones Roalg. Madrid España.

Balestrini, M. 1998. *Cómo se elabora el Proyecto de Investigación en Venezuela.* ED.:Consultores Asociados, Servicio Editorial. Caracas - Venezuela.

Constitución Bolivariana de la República de Venezuela 1999, Disponible en: http://www.analitica.com/bitblioteca/anc/constitucion1999.asp [Consultado Marzo 2007].

Córdova, G. 2004. "*Estudio y comparación de las metodologías ISMS-CMMI*", URL http://weblogs.udp.cl/gcordova/archivos/(861). Trabajo de grado para optar al título de Maestría en Tecnologías de la Información. Universidad Diego Portales. Santiago - Chile. (Consulta: Diciembre 27, 2006).

Corletti, A. 2006. *ISO:27001. Los Controles*. URL: http:// documentos. shellsec. net /otros/iso-27001_los-controles_shellsec.net.pdf (Consulta: Diciembre 27, 2006).

Decreto Ejecutivo No. 3087

Gallo, G.; Coello de Portugal, I.; Larrondo, F.y Sánchez, H. 2003. *La protección de datos personales: Soluciones en entornos Microsoft*. Microsoft Ibérica.

García, P 2005. *¿Dónde nacen las normas voluntarias y las recomendaciones relativas a la seguridad de la información?*. URL: http://www.ati.es/novatica/2005/176/176-7.pdf (Consulta: Enero 10, 2007).

Hamana, J. 2003 *Elementos básicos para modelos de seguridad en organizaciones venezolanas*. Trabajo de grado, Universidad Metropolitana, (UM) Caracas. p. 114.

Hernández, E. 2003. Seguridad y Privacidad en los Sistemas Informáticos. URL: http://www.disca.upv.es/enheror/pdf/ACTASeguridad.PDF (Consulta: Diciembre 27, 2006).

Hernández, R., Fernández, C. y Baptista, P. 2003 *Metodología de la investigación. Tercera* edición. McGraw-Hill Interamericana, S.A. México DF-México.

Hiles, Andrew (2004). *Business Continuity: Best Practices,* Connecticut: Rothstein Associates, Inc

Hurtado, J. 1998. *Metodología de la investigación holistica.* ED.: Fundación Sypal- Fundacite, Caracas – Venezuela.

Hurtado, M. (2.000). *Metodología de la investigación holística*. ED.: SYPAL, Caracas Venezuela

ISO 17799:2005. *Código de Práctica para la Gestión de Seguridad de Información.*

ISO/IEC 13335-1:2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.*

ISO/IEC 27001:2005. *Estándar Internacional. Tecnología de la Información - Técnicas de seguridad - Sistemas de Gestión de Seguridad de la Información – Requerimientos.* Primera Edición 2005 – 10 – 15.

ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards.*

La Academia Latinoamericana de Seguridad Informática (2.004). *Microsoft TechNet modulo de seguridad.* [OnLine] Disponible en: www.mslatam.com/latam/technet/cso/HtmlES/home.asp [consultado octubre 2006].

Ley de Universidades. 1970. Gaceta Oficial No. 1429, Extraordinario, del 8 de septiembre.

Ley Especial contra Delitos Informáticos promulgada en Gaceta Oficial No. 36.920 de fecha 28 de marzo del año 2000 por la Asamblea Nacional, Caracas - Venezuela.

Ley Orgánica de Telecomunicaciones, promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001 por Decreto N° 1.024 - 10 de febrero de 2001, Caracas - Venezuela.

Mendillo, V. 2001. *Seguridad en Informática y Comunicaciones,* [On-Line] Disponible en: http://www./ [consultado Julio 2006].

Moulton, B. 2004. *Administración de la TI y seguridad de la información*, Disponible en http://www.symantec.com/region/mx/enterprisesecurity/content/risks/ LAM_ 3522.html#1 [consultado Marzo 2007]

Navarro, A. 2007. *Metodología para la Gestión de Seguridad de Información en Venezuela.* Trabajo de grado, Universidad Metropolitana (UM), Caracas. p. 88.

OECD. 2002. *Directrices para la seguridad de los sistemas y redes de información – Hacia una cultura de seguridad.* Disponible en: http://www.oecd.org. [Consultado Noviembre 2006].

Ormella, C. (2007). *Gestión y Auditoria de la Seguridad de la Información. Normas ISO 17799:2005 – ISO 27001:2005*. Taller de Implementación basado en una experiencia real.

Peltier, T. (2001). *Information Security Risk Análisis*, Nueva Cork, Auerbach.

Real Academia Española. 2006 [On-Line] Disponible en: http://www.rae.es/ [consultado Julio 2006].

RED, 2002. *Seguridad informática, ¿Qué, porqué y para qué?*. Disponible en http://ciberhabitat.gob.mx/museo/cerquita/redes/ seguridad /intro.htm [consultado Agosto 2006]

Resolución de Consejo Universitario No. 2004-E14-06. *Lineamientos de Tecnología y Servicios de Información de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre"* aprobado el 20 de julio del 2004. Barquisimeto - Venezuela

Resolución de Consejo Universitario No. 2005-E09-05 *Reglamento de Tecnología y Servicios de Información de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre"* aprobado el 04 de Mayo del 2005. Barquisimeto - Venezuela

Revilla, C. y Toubes, L. 2003. "*Evaluación e implantación de un sistema de detección de intrusos para la red académica de la Universidad Católica Andrés Bello*". Trabajo de grado presentado para optar al título de Ingeniero, Universidad Católica Andrés Bello, Caracas – Venezuela.

Ruiz, B. (1.998). *Instrumentos de Investigación Educativa. Procedimiento para su Diseño y Validación.* Ediciones CIDEG, C.A. Barquisimeto.

Santos, Luz. 2001. "*Guía para la evaluación de seguridad en un sistema*", URL http://www.acis.org.co/memorias/JornadasSeguridad/IIJNSI/pamplona.doc. Trabajo de grado para optar al título de Maestría en Ingeniería y Sistemas y Computación, Universidad de Pamplona. Colombia. (Consulta: Diciembre 28, 2006).

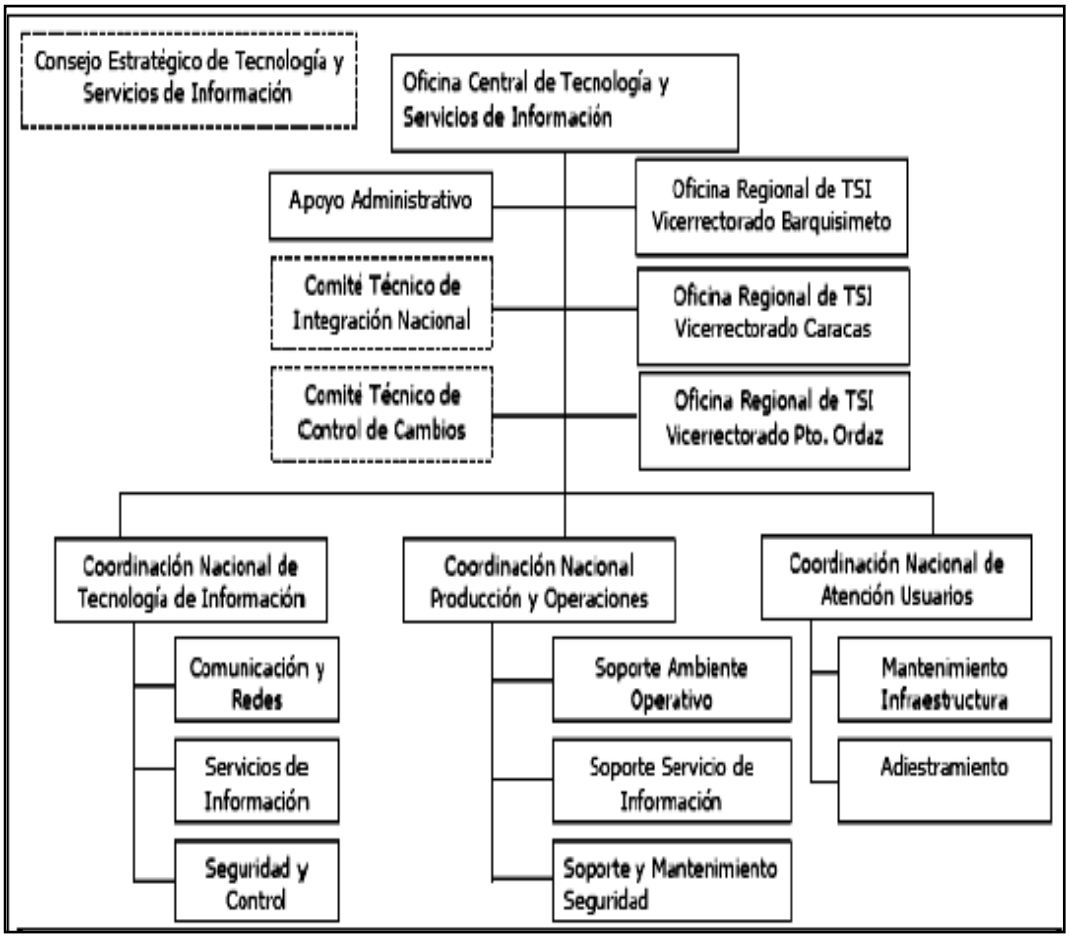
Scott, G. 1988. *Principios de Sistemas de Información.* ED.: McGraw-Hill, Naucalpan de Juárez – México.

Senn, J. 1987. *Análisis y diseño de sistemas de información.* ED.: McGraw-Hill México DF-México.

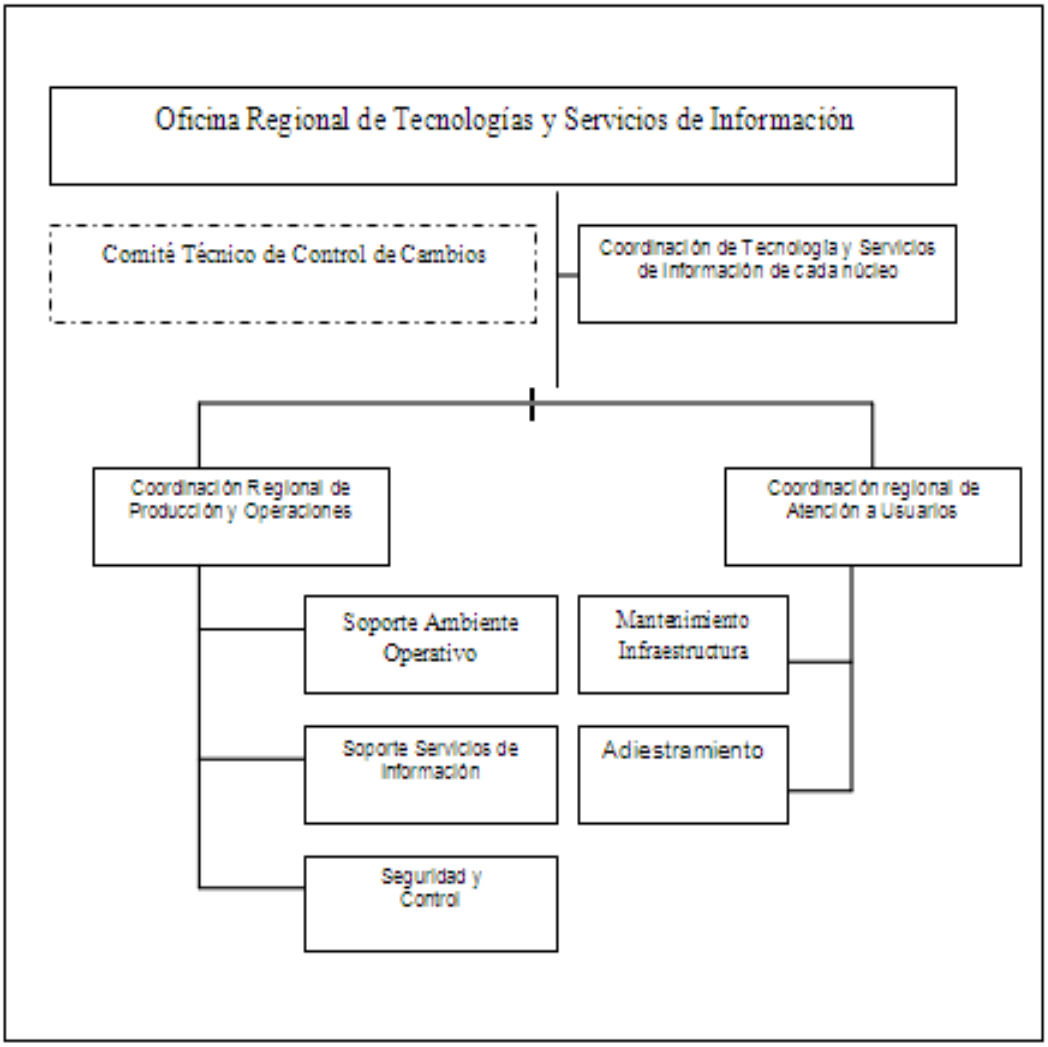
Universidad Centroccidental "Lisandro Alvarado" (UCLA). (2002). *Manual para la Elaboración del Trabajo Conducente al Grado Académico de: Especialización, Maestría y Doctorado.* Barquisimeto – Venezuela.

# ANEXOS

**ANEXO A. ESTRUCTURA ORGANIZATIVA OFICINA CENTRAL DE TECNOLOGÍA Y SERVICIOS DE INFORMACIÓN. OCTSI**.



**ANEXO B. ESTRUCTURA ORGANIZATIVA OFICINA REGIONAL DE TECNOLOGÍA Y SERVICIOS DE INFORMACIÓN. ORTSI.**



## ANEXO C. INSTRUMENTO DE RECOLECCIÓN DE DATOS

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIA Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO
Ciencias de la Computación

### DATOS DEL ENCUESTADO

Nombre y Apellidos: _____

Cargo que desempeña: _____

A quien reporta: _____

Teléfono donde ubicarlo: _____

INFORMACIÓN GENERAL

El presente instrumento fue elaborado para el personal técnico de la Oficina Regional de Tecnología y Servicios de Información (ORTSI) y los usuarios del Sistema Administrativo Integral SAI, específicamente de los departamentos de Dirección Administrativa, Coordinación Administrativa, Presupuesto, Almacén, Compra, Bienes Nacionales, Recursos Humanos, Tesorería y Contabilidad de la Universidad Nacional Experimental "Antonio José de Sucre" (UNEXPO) Vicerrectorado Puerto Ordaz, y tiene como finalidad ayudar a diagnosticar como es la seguridad de la información en la universidad. Las preguntas cubren todos los aspectos de riesgos, incluso las amenazas a la confidencialidad, la integridad y la disponibilidad de los datos, y están estructuradas basándose en los siguientes tópicos:

A. Política de seguridad
B. Organización de la seguridad de la información
C. Gestión de activos
D. Seguridad de recursos humanos
E. Seguridad física y Ambiental
F. Gestión de comunicaciones y operaciones
G. Control de Accesos
H. Adquisición, desarrollo y mantenimiento de sistemas de información

I. Gestión de incidente de seguridad de la información
J. Gestión de continuidad del negocio
K. Cumplimiento

La información obtenida será para uso exclusivo de la investigadora, en el proceso de exploración de las condiciones en que se encuentra la seguridad de la información. Específicamente a través de la investigación se pretende Diseñar un Sistema de Gestión de la Seguridad de la Información para la UNEXPO, Vicerrectorado de Puerto Ordaz, por lo que se le agradece la mayor objetividad posible, recuerde que su colaboración permitirá el logro de los objetivos de la investigación.

Muchas Gracias por su Colaboración.

***Yaneisy Tersek***

**INSTRUCCIONES:**

1. Lea cuidadosamente cada uno de los planteamientos
2. Marque con una equis (X) en el espacio correspondiente, la alternativa que más se ajuste a su criterio y a lo que Usted considere que ocurre en la Universidad.
3. Las alternativas de respuestas son cinco (5), considerando la siguiente escala.

| Siempre | Casi Siempre | Algunas Veces | Casi Nunca | Nunca |
|---|---|---|---|---|
| **S** | **CS** | **AV** | **CN** | **N** |

4. Seleccione solo una alternativa para cada uno de los planteamientos.

| Siempre | Casi Siempre | Algunas Veces | Casi Nunca | Nunca |
|---|---|---|---|---|
| **S** | **CS** | **AV** | **CN** | **N** |

| **ÍTEMS** | **S** | **CS** | **AV** | **CN** | **N** |
|---|---|---|---|---|---|
| **POLÍTICAS DE SEGURIDAD**<br>1. ¿Existe una preocupación dentro de la UNEXPO por la elaboración de un documento de políticas de seguridad de información con los procedimientos a seguir para cada uno de los riesgos más graves que tiene la información? | | | | | |
| 2. ¿Se toman acciones rápidas y correctivas cuando la información está en peligro? | | | | | |
| 3. ¿Se revisan periódicamente las medidas y procedimientos de seguridad para determinar si son efectivos? | | | | | |
| **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**<br>4 ¿El Vicerrector regional y los jefes de las diferentes unidades administrativas del Vicerrectorado de Puerto Ordaz entienden, apoyan y llevan a cabo eficazmente políticas de seguridad de la información dentro la Universidad? | | | | | |
| 5. ¿La UNEXPO se preocupa de que el personal tome consciencia sobre la importancia de la seguridad de la información y sus responsabilidades individuales para alcanzarla? | | | | | |
| 6. ¿Se definen claramente todas las responsabilidades entorno a la seguridad de la información? | | | | | |
| 7. ¿Se define e implementa un proceso de autorización para los recursos de procesamiento de la información? | | | | | |
| 8. ¿Se definen los requisitos para los acuerdos de confidencialidad o no divulgación de la información? | | | | | |
| 9. ¿Se tienen previstos mecanismos de seguridad para preservar la información de intervenciones externas? | | | | | |
| 10. ¿Se consideran todos los requisitos de seguridad identificados antes de dar el acceso al cliente o usuario a la información o posesiones de la universidad? | | | | | |

| Siempre | Casi Siempre | Algunas Veces | Casi Nunca | Nunca |
|---|---|---|---|---|
| **S** | **CS** | **AV** | **CN** | **N** |

| ITEMS | S | CS | AV | CN | N |
|---|---|---|---|---|---|
| **GESTIÓN DE ACTIVOS**<br>11. ¿Se identifican los equipos de computación, tales como: laptops, computadoras de escritorio y otros, con el nombre de la Universidad, nombre del departamento u oficina, teléfono, serial del equipo, serial de bienes nacionales, entre otros? | | | | | |
| 12. ¿Se realizan inventarios en cada oficina o unidad administrativa de los equipos informáticos y de comunicaciones, con el serial del equipo, software instalados, usuario asignado, ubicación, entre otros? | | | | | |
| 13. ¿Se identifican todos los activos de información para conocer su contenido y a qué departamento pertenecen? | | | | | |
| 14. ¿Se dan directrices para clasificar la información de acuerdo con su valor, requisitos legales, sensibilidad y criticidad para la universidad? | | | | | |
| **SEGURIDAD DE RECURSOS HUMANOS**<br>15. ¿Se realiza una verificación de los antecedentes de los candidatos para ocupar cargos administrativos, contratistas y usuarios de terceras partes de acuerdo con las leyes, reglamentaciones y ética pertinentes a los requisitos de la Universidad, clasificación de información a ser accesada y los riesgos percibidos? | | | | | |
| 16. ¿La Universidad aplica procesos disciplinarios a los funcionarios que cometan un incumplimiento de seguridad? | | | | | |
| 17. ¿Se vigilan la moral y el comportamiento del personal que maneja los sistemas de información con el fin de mantener una buena imagen y evitar un posible fraude? | | | | | |
| 18. ¿Se retiran los derechos de acceso a todos los empleados, contratistas y usuarios de terceras partes a la información y al recurso para el procesamiento de la información una vez terminado su empleo, contrato o acuerdo, o una vez ajustado el cambio a otra dependencia? | | | | | |
| 19. ¿La Universidad se asegura de que los empleados, contratista y usuarios de terceras partes devuelvan todos los activos de la Universidad que posean una vez terminado su empleo, contrato o acuerdo? | | | | | |

| Siempre | Casi Siempre | Algunas Veces | Casi Nunca | Nunca |
|---|---|---|---|---|
| **S** | **CS** | **AV** | **CN** | **N** |

| **ITEMS** | **S** | **CS** | **AV** | **CN** | **N** |
|---|---|---|---|---|---|
| **SEGURIDAD FÍSICA Y AMBIENTAL** | | | | | |
| 20. ¿En la Universidad se establecen adecuadamente los perímetros de seguridad (barreras tales cómo paredes, puertas de entradas controladas por tarjetas o puesto de recepción manual) a las áreas que contienen la información y las instalaciones de procesamiento de la información? | | | | | |
| 21. ¿Se diseñan y aplican controles de entradas apropiados a las áreas de seguridad a fin de asegurar el permiso de acceso sólo al personal autorizado? | | | | | |
| 22. ¿Existe un procedimiento o control de admisión al edificio administrativo para aquellas personas que no posean carnet institucional, tal como los visitantes? | | | | | |
| 23. ¿Se controla el ingreso a las oficinas después del horario normal de trabajo? | | | | | |
| 24. ¿Se cierran con llave las puertas de los sitios neurálgicos en el edificio administrativo? | | | | | |
| 25. ¿Se cierran con llaves las entradas de cada piso, asi cómo las entradas externas al edificio administrativo? | | | | | |
| 26. ¿Se diseñan y aplican protección física a las oficinas contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre? | | | | | |
| 27. ¿Se diseñan y aplican protección física a la información contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre? | | | | | |
| 28. ¿La Universidad toma medidas concretas para evitar el robo de equipos tales como laptops y otros componentes? | | | | | |
| 29. ¿Se toman previsiones de ubicar o proteger los equipos para reducir los riesgos de amenazas y peligros ambientales, y oportunidades para el acceso no autorizado? | | | | | |
| 30. ¿Se protegen los equipos contra fallas de energía y otras interrupciones eléctricas causadas por problemas en los servicios de apoyo? | | | | | |

| Siempre | Casi Siempre | Algunas Veces | Casi Nunca | Nunca |
|---|---|---|---|---|
| **S** | **CS** | **AV** | **CN** | **N** |

| **ITEMS** | **S** | **CS** | **AV** | **CN** | **N** |
|---|---|---|---|---|---|
| 31. ¿Se protegen debidamente el cableado de energía eléctrica y de comunicaciones que transporta datos contra la interceptación o daños? | | | | | |
| 32. ¿Se realizan mantenimientos preventivos a los equipos a fin de asegurar su continua disponibilidad e integridad? | | | | | |
| 33. ¿Se toman las previsiones para que todos los dispositivos de almacenamiento de datos (Pendrive, CD, Disquette, Disco duros, entre otros), sean eliminados o formateado completamente ante de su disposición? | | | | | |
| 34. ¿La UNEXPO da instrucciones claras y firmes a los vigilantes para que prohiban el traslado o retiro de equipo, información o software sin autorización? | | | | | |
| **GESTIÓN DE COMUNICACIONES Y OPERACIONES**<br>35. ¿Los procedimientos operativos son documentados, mantenidos y están disponibles a todos los usuarios que lo necesitan? | | | | | |
| 36. ¿Se controlan los cambios de los recursos y sistemas de procesamiento de la información? | | | | | |
| 37. ¿Se realizan seguimientos, ajustes y proyecciones de los requisitos de la capacidad futura de la utilización de los recursos, para garantizar el desempeño del sistema requerido? | | | | | |
| 38. ¿Se implementan controles de detección, prevención y recuperación de la información, para la protección contra código malicioso o virus? | | | | | |
| 39. ¿Se realizan procedimientos adecuados de toma de conciencia de los usuarios para la detección, prevención y recuperación para la protección contra código malicioso? | | | | | |
| 40. ¿Se establecen procedimientos para controlar el intercambio de información a través de la utilización de toda clase de recursos de comunicación, por ejemplo el uso de teléfonos celulares y laptops por parte de personas ajenas a la universidad? | | | | | |
| 41. ¿Se controla el acceso a las fotocopiadoras para evitar que se puedan hacer copias de cualquier documento? | | | | | |

| Siempre | Casi Siempre | Algunas Veces | Casi Nunca | Nunca |
|---|---|---|---|---|
| **S** | **CS** | **AV** | **CN** | **N** |

| **ITEMS** | **S** | **CS** | **AV** | **CN** | **N** |
|---|---|---|---|---|---|
| 42. ¿Se realizan copias de seguridad de la información y software de acuerdo con la política de copia de seguridad acordada? | | | | | |
| 43. ¿Se gestionan y controlan adecuadamente la red de datos a fin de protegerla de las amenazas y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la información en tránsito? | | | | | |
| 44. ¿Se tiene el cuidado de no botar información confidencial o vital en las papeleras sin ser destruida previamente? | | | | | |
| 45. ¿Se establecen procedimientos para el manejo y almacenamiento de la información a fin de protegerla contra su uso inadecuado o divulgación no autorizada? | | | | | |
| 46. ¿Se producen y mantienen los registros de auditorias cuando se detectan actividades de procesamiento de la información no autorizada, a fin de ayudar a futuras investigaciones y seguimiento de control de accesos? | | | | | |
| 47. ¿Se registran, analizan y se toman acciones apropiadas cuando se detectan fallas en las actividades y procesamiento de la información no autorizada? | | | | | |
| 48. ¿Se sincronizan los relojes de todos los sistemas de procesamiento de la información pertinentes dentro de la universidad con una fuente de tiempo exacta acordada? | | | | | |
| **CONTROL DE ACCESOS**<br>49. ¿Se establecen, documentan y revisan las políticas de control de accesos a la información? | | | | | |
| 50. ¿Se realizan procedimientos formales de registros y des-registros de usuarios para conceder y revocar el acceso a los sistemas y servicios de información? | | | | | |
| 51. ¿Se controla a través de un proceso de gestión formal la asignación de contraseñas de usuarios para prevenir el acceso no autorizado a los sistemas de información? | | | | | |
| 52. ¿Se le motiva a los usuarios seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas? | | | | | |

| Siempre | Casi Siempre | Algunas Veces | Casi Nunca | Nunca |
|---|---|---|---|---|
| **S** | **CS** | **AV** | **CN** | **N** |

| **ITEMS** | **S** | **CS** | **AV** | **CN** | **N** |
|---|---|---|---|---|---|
| 53. ¿Se activa automáticamente un protector de pantalla protegido con contraseña, cuando el usuario deja de utilizar un tiempo prudencial la máquina? | | | | | |
| 54. ¿Se restringue de acuerdo con la políticas de control el acceso a la información y a las funciones del sistema de aplicación? | | | | | |
| **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**<br>55. ¿Se realizan análisis y especificaciones de seguridad para los nuevos sistemas de información o para las mejoras de los sistemas existentes? | | | | | |
| 56. ¿Se realizan validaciones de los datos de entrada a las aplicaciones para asegurarse de que éstos sean correctos y apropiados? | | | | | |
| 57. ¿Se incorporan a las aplicaciones las comprobaciones de validación para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados? | | | | | |
| 58. ¿Se realizan validaciones a los datos de salida de una aplicación para asegurarse que el procedimiento de la información almacenada es correcto y apropiado a las circunstancias? | | | | | |
| 59. ¿Se desarrollan e implementan políticas sobre la utilización de controles para la protección de confidencialidad, autenticidad o integridad de la información? | | | | | |
| **GESTIÓN DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN**<br>60. ¿Se reportan los eventos de seguridad de la información a través de los canales de gestión apropiados tan rápidamente cómo sea posible? | | | | | |

| Siempre | Casi Siempre | Algunas Veces | Casi Nunca | Nunca |
|---|---|---|---|---|
| **S** | **CS** | **AV** | **CN** | **N** |

| **ITEMS** | **S** | **CS** | **AV** | **CN** | **N** |
|---|---|---|---|---|---|
| 61. ¿Se les solicita a todos los usuarios de los sistemas y servicios de información reportar cualquier debilidad en la seguridad de los sistemas o servicios, que haya sido observada o sospechada? | | | | | |
| 62. ¿Se establecen las responsabilidades y procedimiento de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información? | | | | | |
| 63. ¿Se establecen mecanismos que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de seguridad de información? | | | | | |
| **GESTIÓN DE CONTINUIDAD DEL NEGOCIO**<br>64. ¿Se identifican los eventos que pueden causar las interrupciones a los procesos de la universidad, al mismo tiempo que la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información? | | | | | |
| 65. ¿Se desarrollan e implementan planes para mantener y recuperar las operaciones y asegurar la disponibilidad de la información al nivel requerido y en los plazos requeridos, tras la interrupción o la falla de los procesos críticos de la Universidad? | | | | | |
| **CUMPLIMIENTO**<br>66. ¿Se definen, documentan y se actualizan todos los requisitos legales, reglamentarios y contractuales para cada sistema de información de la universidad? | | | | | |
| 67. ¿Se implementa procedimientos apropiados para asegurarse del cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material protegido por derechos de propiedad intelectual, y sobre el uso de productos de software reservados? | | | | | |
| 68. ¿Se protegen los registros importantes contra pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales de la universidad? | | | | | |
| 69. ¿Se planifican actividades de auditorias que involucren comprobaciones en los sistemas operativos y sistemas de información a fin de minimizar el riesgo de interrupción de los procesos de la universidad? | | | | | |

**ANEXO D. FORMATO PARA LA REVISIÓN Y VALIDACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS**

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIA Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO
Maestría en Ciencias de la Computación

Señor(a):

_____
Ciudad.

Por medio de la presente, me dirijo a Usted, como experto en el área, para informarle, que ha sido seleccionado (a) para la validación del instrumento a utilizar en el desarrollo de la investigación, la cual se titula: **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UN SISTEMA DE INFORMACIÓN (Caso de estudio: Sistema Administrativo Integrado SAI en la Red de datos de la UNEXPO- Puerto Ordaz)**

A tal fin, se anexa cuadro de operacionalización de variables, los instrumentos de recolección de datos y el respectivo formato de revisión y validación, además del objetivo general y los objetivos específicos de la investigación.

Se debe resaltar, en cuanto a la investigación, que la misma es una investigación de campo, con modalidad de proyecto factible.

Sin más a que hacer referencia y agradeciendo su mayor colaboración al respecto,

Atentamente

***Yaneisy Tersek***

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIA Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO
Maestría en Ciencias de la Computación

**INSTRUCCIONES**

- Lea detenidamente cada uno de los ítems relacionados con cada indicador.
- Utilice este formato para indicar su grado de acuerdo con cada enunciado que se presenta, marcando con una equis (X), en el espacio correspondiente.

- Si desea plantear alguna observación para mejorar el instrumento, utilice el espacio correspondiente a observaciones ubicado en el margen derecho.

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| 1 | **POLÍTICAS DE SEGURIDAD**<br>¿Existe una preocupación dentro de la UNEXPO por la elaboración de un documento de políticas de seguridad de información con los procedimientos a seguir para cada uno de los riesgos más graves que tiene la información? | | | | | | | |
| 2 | ¿Se toman acciones rápidas y correctivas cuando la información está en peligro? | | | | | | | |
| 3 | ¿Se revisan periódicamente las medidas y procedimientos de seguridad para determinar si son efectivos? | | | | | | | |
| 4 | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**<br>¿El Vicerrector regional y los jefes de las diferentes unidades administrativas del Vicerrectorado de Puerto Ordaz entienden, apoyan y llevan a cabo eficazmente políticas de seguridad de la información dentro la Universidad? | | | | | | | |
| 5 | ¿La UNEXPO se preocupa de que el personal tome consciencia sobre la importancia de la seguridad de la información y sus responsabilidades individuales | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | para alcanzarla? | | | | | | | |
| 6 | ¿Se definen claramente todas las responsabilidades en torno a la seguridad de la información? | | | | | | | |
| 7 | ¿Se define e implementa un proceso de autorización para los recursos de procesamiento de la información? | | | | | | | |
| 8 | ¿Se definen los requisitos para los acuerdos de confidencialidad o no divulgación de la información? | | | | | | | |
| 9 | ¿Se tienen previstos mecanismos de seguridad para preservar la información de intervenciones externas? | | | | | | | |
| 10 | ¿Se consideran todos los requisitos de seguridad identificados antes de dar el acceso al cliente o usuario a la información o posesiones de la universidad? | | | | | | | |
| 11 | **GESTIÓN DE ACTIVOS**<br>¿Se identifican los equipos de computación, tales como: laptops, computadoras de escritorio y otros, | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | con el nombre de la Universidad, nombre del departamento u oficina, teléfono, serial del equipo, serial de bienes nacionales, entre otros? | | | | | | | |
| 12 | ¿Se realizan inventarios en cada oficina o unidad administrativa de los equipos informáticos y de comunicaciones, con el serial del equipo, software instalados, usuario asignado, ubicación, entre otros? | | | | | | | |
| 13 | ¿Se identifican todos los activos de información para conocer su contenido y a qué departamento pertenecen? | | | | | | | |
| 14 | ¿Se dan directrices para clasificar la información de acuerdo con su valor, requisitos legales, sensibilidad y criticidad para la universidad? | | | | | | | |
| 15 | **SEGURIDAD DE RECURSOS HUMANOS**<br>¿Se realiza una verificación de los antecedentes de los candidatos para ocupar cargos administrativos, contratistas y usuarios de terceras partes de acuerdo con las leyes, reglamentaciones y ética pertinentes a los requisitos de la Universidad, clasificación de información a ser accesada y los riesgos | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | percibidos? | | | | | | | |
| 16 | ¿La Universidad aplica procesos disciplinarios a los funcionarios que cometan un incumplimiento de seguridad? | | | | | | | |
| 17 | ¿Se vigilan la moral y el comportamiento del personal que maneja los sistemas de información con el fin de mantener una buena imagen y evitar un posible fraude? | | | | | | | |
| 18 | ¿Se retiran los derechos de acceso a todos los empleados, contratistas y usuarios de terceras partes a la información y al recurso para el procesamiento de la información una vez terminado su empleo, contrato o acuerdo, o una vez ajustado el cambio a otra dependencia? | | | | | | | |
| 19 | ¿La Universidad se asegura de que los empleados, contratista y usuarios de terceras partes devuelvan todos los activos de la Universidad que posean una vez terminado su empleo, contrato o acuerdo? | | | | | | | |
| 20 | **SEGURIDAD FÍSICA Y AMBIENTAL**<br>¿En la Universidad se establecen adecuadamente | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | los perímetros de seguridad (barreras tales cómo paredes, puertas de entradas controladas por tarjetas o puesto de recepción manual) a las áreas que contienen la información y las instalaciones de procesamiento de la información? | | | | | | | |
| 21 | ¿Se diseñan y aplican controles de entradas apropiados a las áreas de seguridad a fin de asegurar el permiso de acceso sólo al personal autorizado? | | | | | | | |
| 22 | ¿Existe un procedimiento o control de admisión al edificio administrativo para aquellas personas que no posean carnet institucional, tal como los visitantes? | | | | | | | |
| 23 | ¿Se controla el ingreso a las oficinas después del horario normal de trabajo? | | | | | | | |
| 24 | ¿Se cierran con llave las puertas de los sitios neurálgicos en el edificio administrativo? | | | | | | | |
| 25 | ¿Se cierran con llaves las entradas de cada piso, asi cómo las entradas externas al edificio administrativo? | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| 26 | ¿Se diseñan y aplican protección física a las oficinas contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre? | | | | | | | |
| 27 | ¿Se diseñan y aplican protección física a la información contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre? | | | | | | | |
| 28 | ¿La Universidad toma medidas concretas para evitar el robo de equipos tales como laptops y otros componentes? | | | | | | | |
| 29 | ¿Se toman previsiones de ubicar o proteger los equipos para reducir los riesgos de amenazas y peligros ambientales, y oportunidades para el acceso no autorizado? | | | | | | | |
| 30 | ¿Se protegen los equipos contra fallas de energía y otras interrupciones eléctricas causadas por problemas en los servicios de apoyo? | | | | | | | |
| 31 | ¿Se protegen debidamente el cableado de energía eléctrica y de comunicaciones que transporta datos | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | contra la interceptación o daños? | | | | | | | |
| 32 | ¿Se realizan mantenimientos preventivos a los equipos a fin de asegurar su continua disponibilidad e integridad? | | | | | | | |
| 33 | ¿Se toman las previsiones para que todos los dispositivos de almacenamiento de datos (Pendrive, CD, Disquette, Disco duros, entre otros), sean eliminados o formateado completamente ante de su disposición? | | | | | | | |
| 34 | ¿La UNEXPO da instrucciones claras y firmes a los vigilantes para que prohiban el traslado o retiro de equipo, información o software sin autorización? | | | | | | | |
| 35 | **GESTIÓN DE COMUNICACIONES Y OPERACIONES**<br>¿Los procedimientos operativos son documentados, mantenidos y están disponibles a todos los usuarios que lo necesitan? | | | | | | | |
| 36 | ¿Se controlan los cambios de los recursos y sistemas de procesamiento de la información? | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| 37 | ¿Se realizan seguimientos, ajustes y proyecciones de los requisitos de la capacidad futura de la utilización de los recursos, para garantizar el desempeño del sistema requerido? | | | | | | | |
| 38 | ¿Se implementan controles de detección, prevención y recuperación de la información, para la protección contra código malicioso o virus? | | | | | | | |
| 39 | ¿Se realizan procedimientos adecuados de toma de conciencia de los usuarios para la detección, prevención y recuperación para la protección contra código malicioso? | | | | | | | |
| 40 | ¿Se establecen procedimientos para controlar el intercambio de información a través de la utilización de toda clase de recursos de comunicación, por ejemplo el uso de teléfonos celulares y laptops por parte de personas ajenas a la universidad? | | | | | | | |
| 41 | ¿Se controla el acceso a las fotocopiadoras para evitar que se puedan hacer copias de cualquier documento? | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| 42 | ¿Se realizan copias de seguridad de la información y software de acuerdo con la política de copia de seguridad acordada? | | | | | | | |
| 43 | ¿Se gestionan y controlan adecuadamente la red de datos a fin de protegerla de las amenazas y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la información en tránsito? | | | | | | | |
| 44 | ¿Se tiene el cuidado de no botar información confidencial o vital en las papeleras sin ser destruida previamente? | | | | | | | |
| 46 | ¿Se establecen procedimientos para el manejo y almacenamiento de la información a fin de protegerla contra su uso inadecuado o divulgación no autorizada? | | | | | | | |
| 47 | ¿Se producen y mantienen los registros de auditorias cuando se detectan actividades de procesamiento de la información no autorizada, a fin de ayudar a futuras investigaciones y seguimiento de control de accesos? | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| 48 | ¿Se registran, analizan y se toman acciones apropiadas cuando se detectan fallas en las actividades y procesamiento de la información no autorizada? | | | | | | | |
| 49 | ¿Se sincronizan los relojes de todos los sistemas de procesamiento de la información pertinentes dentro de la universidad con una fuente de tiempo exacta acordada? | | | | | | | |
| 50 | **CONTROL DE ACCESOS**<br>¿Se establecen, documentan y revisan las políticas de control de accesos a la información? | | | | | | | |
| 51 | ¿Se realizan procedimientos formales de registros y des-registros de usuarios para conceder y revocar el acceso a los sistemas y servicios de información? | | | | | | | |
| 52 | ¿Se controla a través de un proceso de gestión formal la asignación de contraseñas de usuarios para prevenir el acceso no autorizado a los sistemas de información? | | | | | | | |
| 53 | ¿Se les motiva a los usuarios seguir buenas prácticas de seguridad para la selección y uso de | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | sus contraseñas? | | | | | | | |
| 54 | ¿Se activa automáticamente un protector de pantalla protegido con contraseña, cuando el usuario deja de utilizar un tiempo prudencial la máquina? | | | | | | | |
| 55 | ¿Se restringue de acuerdo con la políticas de control el acceso a la información y a las funciones del sistema de aplicación? | | | | | | | |
| 56 | **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**<br>¿Se realizan análisis y especificaciones de seguridad para los nuevos sistemas de información o para las mejoras de los sistemas existentes? | | | | | | | |
| 57 | ¿Se realizan validaciones de los datos de entrada a las aplicaciones para asegurarse de que éstos sean correctos y apropiados? | | | | | | | |
| 58 | ¿Se incorporan a las aplicaciones las comprobaciones de validación para detectar cualquier corrupción de la información a través de | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | errores de procesamiento o actos deliberados? | | | | | | | |
| 59 | ¿Se realizan validaciones a los datos de salida de una aplicación para asegurarse que el procedimiento de la información almacenada es correcto y apropiado a las circunstancias? | | | | | | | |
| 60 | ¿Se desarrollan e implementan políticas sobre la utilización de controles para la protección de confidencialidad, autenticidad o integridad de la información? | | | | | | | |
| 61 | **GESTIÓN DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** ¿Se reportan los eventos de seguridad de la información a través de los canales de gestión apropiados tan rápidamente cómo sea posible? | | | | | | | |
| 62 | ¿Se les solicita a todos los usuarios de los sistemas y servicios de información reportar cualquier debilidad en la seguridad de los sistemas o servicios, que haya sido observada o sospechada? | | | | | | | |
| 63 | ¿Se establecen las responsabilidades y procedimiento de gestión para asegurar una | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información? | | | | | | | |
| 64 | ¿Se establecen mecanismos que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de seguridad de información? | | | | | | | |
| 65 | **GESTIÓN DE CONTINUIDAD DEL NEGOCIO**<br>¿Se identifican los eventos que pueden causar las interrupciones a los procesos de la universidad, al mismo tiempo que la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información? | | | | | | | |
| 66 | ¿Se desarrollan e implementan planes para mantener y recuperar las operaciones y asegurar la disponibilidad de la información al nivel requerido y en los plazos requeridos, tras la interrupción o la falla de los procesos críticos de la universidad? | | | | | | | |
| 67 | **CUMPLIMIENTO**<br>¿Se definen, documentan y se actualizan todos los requisitos legales, reglamentarios y contractuales | | | | | | | |

| Ítem | Pregunta | Claridad | | Congruencia | | Redacción | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | Si | No | Si | No | Si | No | |
| | para cada sistema de información de la universidad? | | | | | | | |
| 68 | ¿Se implementa procedimientos apropiados para asegurarse del cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material protegido por derechos de propiedad intelectual, y sobre el uso de productos de software reservados? | | | | | | | |
| 69 | ¿Se protegen los registros importantes contra pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales de la universidad? | | | | | | | |
| 70 | ¿Se planifican actividades de auditorias que involucren comprobaciones en los sistemas operativos y sistemas de información a fin de minimizar el riesgo de interrupción de los procesos de la universidad? | | | | | | | |

## ANEXO E. CALCULO DE LA CONFIABILIDAD. MÉTODO ALPHA DE CROMBACH

| Sujetos / Ítems | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Sumatoria | Media | Varianza | Desv. Típica |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 4 | 2 | 1 | 3 | 3 | 4 | 1 | 1 | 1 | 21 | 2,1 | 1,7 | 1,2 |
| 2 | 1 | 4 | 5 | 3 | 2 | 4 | 3 | 4 | 2 | 2 | 30 | 3,0 | 1,6 | 1,2 |
| 3 | 1 | 2 | 2 | 2 | 2 | 3 | 4 | 2 | 1 | 1 | 20 | 2,0 | 0,9 | 0,9 |
| 4 | 2 | 3 | 2 | 2 | 3 | 3 | 3 | 2 | 1 | 1 | 22 | 2,2 | 0,6 | 0,7 |
| 5 | 2 | 3 | 4 | 3 | 3 | 4 | 3 | 3 | 1 | 1 | 27 | 2,7 | 1,1 | 1 |
| 6 | 3 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 1 | 2 | 25 | 2,5 | 0,5 | 0,7 |
| 7 | 2 | 2 | 5 | 3 | 3 | 1 | 3 | 1 | 2 | 2 | 24 | 2,4 | 1,4 | 1,1 |
| 8 | 2 | 2 | 2 | 5 | 2 | 1 | 3 | 2 | 2 | 1 | 22 | 2,2 | 1,3 | 1,1 |
| 9 | 3 | 4 | 4 | 5 | 2 | 1 | 3 | 1 | 1 | 2 | 26 | 2,6 | 2 | 1,4 |
| 10 | 2 | 5 | 4 | 5 | 2 | 1 | 3 | 4 | 3 | 2 | 31 | 3,1 | 1,9 | 1,3 |
| 11 | 3 | 3 | 2 | 1 | 2 | 5 | 4 | 4 | 1 | 1 | 26 | 2,6 | 2 | 1,4 |
| 12 | 3 | 2 | 5 | 4 | 4 | 4 | 4 | 5 | 4 | 3 | 38 | 3,8 | 0,8 | 0,9 |
| 13 | 3 | 2 | 5 | 5 | 2 | 3 | 4 | 5 | 4 | 3 | 36 | 3,6 | 1,4 | 1,1 |
| 14 | 1 | 1 | 4 | 4 | 2 | 2 | 3 | 4 | 3 | 3 | 27 | 2,7 | 1,3 | 1,1 |
| 15 | 3 | 1 | 2 | 3 | 2 | 1 | 4 | 5 | 2 | 2 | 25 | 2,5 | 1,6 | 1,2 |
| 16 | 3 | 4 | 2 | 2 | 2 | 1 | 3 | 3 | 2 | 2 | 24 | 2,4 | 0,7 | 0,8 |
| 17 | 3 | 4 | 2 | 5 | 2 | 1 | 4 | 3 | 2 | 2 | 28 | 2,8 | 1,5 | 1,2 |
| 18 | 4 | 3 | 4 | 1 | 2 | 1 | 3 | 2 | 2 | 2 | 24 | 2,4 | 1,2 | 1 |
| 19 | 2 | 3 | 3 | 5 | 2 | 1 | 3 | 4 | 3 | 3 | 29 | 2,9 | 1,2 | 1 |
| 20 | 4 | 3 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 16 | 1,6 | 1,2 | 1 |
| 21 | 2 | 2 | 2 | 1 | 2 | 3 | 3 | 2 | 1 | 2 | 20 | 2,0 | 0,4 | 0,6 |
| 22 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 13 | 1,3 | 0,2 | 0,5 |
| 23 | 2 | 4 | 4 | 4 | 3 | 3 | 1 | 2 | 4 | 3 | 30 | 3,0 | 1,1 | 1 |
| 24 | 4 | 4 | 5 | 5 | 3 | 3 | 2 | 1 | 3 | 3 | 33 | 3,3 | 1,6 | 1,2 |
| 25 | 1 | 4 | 1 | 3 | 3 | 4 | 2 | 2 | 2 | 2 | 24 | 2,4 | 1,2 | 1 |
| 26 | 1 | 3 | 3 | 1 | 2 | 1 | 1 | 2 | 2 | 2 | 18 | 1,8 | 0,6 | 0,7 |
| 27 | 1 | 3 | 1 | 1 | 2 | 1 | 1 | 2 | 4 | 4 | 20 | 2,0 | 1,6 | 1,2 |
| 28 | 1 | 2 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 2 | 16 | 1,6 | 0,3 | 0,5 |
| 29 | 1 | 2 | 3 | 5 | 2 | 3 | 1 | 1 | 4 | 4 | 26 | 2,6 | 2 | 1,4 |
| 30 | 2 | 1 | 2 | 5 | 3 | 3 | 1 | 2 | 4 | 4 | 27 | 2,7 | 1,8 | 1,3 |
| 31 | 2 | 2 | 2 | 1 | 3 | 1 | 1 | 2 | 3 | 3 | 20 | 2,0 | 0,7 | 0,8 |
| 32 | 3 | 2 | 4 | 5 | 2 | 3 | 2 | 2 | 4 | 4 | 31 | 3,1 | 1,2 | 1 |
| 33 | 3 | 5 | 2 | 3 | 2 | 3 | 2 | 2 | 3 | 3 | 28 | 2,8 | 0,8 | 0,9 |
| 34 | 3 | 4 | 5 | 5 | 2 | 1 | 3 | 2 | 1 | 1 | 27 | 2,7 | 2,5 | 1,5 |
| 35 | 3 | 3 | 2 | 3 | 1 | 3 | 2 | 1 | 3 | 4 | 25 | 2,5 | 0,9 | 0,9 |
| 36 | 3 | 2 | 3 | 5 | 3 | 1 | 2 | 2 | 3 | 4 | 28 | 2,8 | 1,3 | 1,1 |

| Sujetos / Ítems | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Sumatoria | Media | Varianza | Desv. Típica |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 37 | 3 | 2 | 2 | 4 | 3 | 1 | 2 | 2 | 2 | 2 | 23 | 2,3 | 0,7 | 0,8 |
| 38 | 3 | 2 | 5 | 5 | 3 | 1 | 2 | 2 | 1 | 1 | 25 | 2,5 | 2,3 | 1,4 |
| 39 | 3 | 3 | 4 | 4 | 2 | 1 | 2 | 2 | 2 | 2 | 25 | 2,5 | 0,9 | 0,9 |
| 40 | 2 | 2 | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 2 | 16 | 1,6 | 0,3 | 0,5 |
| 41 | 2 | 1 | 3 | 1 | 1 | 1 | 1 | 3 | 2 | 2 | 17 | 1,7 | 0,7 | 0,8 |
| 42 | 3 | 4 | 4 | 2 | 4 | 1 | 2 | 2 | 1 | 1 | 24 | 2,4 | 1,6 | 1,2 |
| 43 | 3 | 4 | 1 | 5 | 3 | 1 | 2 | 2 | 1 | 1 | 23 | 2,3 | 2 | 1,3 |
| 44 | 1 | 4 | 5 | 2 | 2 | 1 | 3 | 2 | 2 | 2 | 24 | 2,4 | 1,6 | 1,2 |
| 45 | 1 | 3 | 5 | 5 | 3 | 1 | 3 | 2 | 1 | 1 | 25 | 2,5 | 2,5 | 1,5 |
| 46 | 1 | 2 | 1 | 1 | 3 | 2 | 2 | 2 | 3 | 3 | 20 | 2,0 | 0,7 | 0,8 |
| 47 | 2 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 16 | 1,6 | 0,3 | 0,5 |
| 48 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 14 | 1,4 | 0,3 | 0,5 |
| 49 | 2 | 1 | 1 | 3 | 2 | 1 | 2 | 1 | 3 | 3 | 19 | 1,9 | 0,8 | 0,8 |
| 50 | 2 | 2 | 2 | 4 | 2 | 2 | 2 | 1 | 3 | 3 | 23 | 2,3 | 0,7 | 0,8 |
| 51 | 2 | 3 | 1 | 5 | 2 | 2 | 2 | 4 | 3 | 3 | 27 | 2,7 | 1,3 | 1,1 |
| 52 | 3 | 3 | 3 | 5 | 2 | 1 | 2 | 4 | 2 | 2 | 27 | 2,7 | 1,3 | 1,1 |
| 53 | 3 | 2 | 1 | 1 | 2 | 1 | 3 | 2 | 2 | 2 | 19 | 1,9 | 0,5 | 0,7 |
| 54 | 3 | 2 | 2 | 3 | 2 | 1 | 2 | 2 | 2 | 2 | 21 | 2,1 | 0,3 | 0,5 |
| 55 | 3 | 5 | 1 | 5 | 2 | 3 | 3 | 2 | 2 | 2 | 28 | 2,8 | 1,7 | 1,2 |
| 56 | 3 | 5 | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 2 | 31 | 3,1 | 1 | 0,9 |
| 57 | 3 | 3 | 1 | 3 | 3 | 3 | 3 | 4 | 2 | 2 | 27 | 2,7 | 0,7 | 0,8 |
| 58 | 3 | 2 | 1 | 3 | 3 | 1 | 3 | 2 | 2 | 1 | 21 | 2,1 | 0,8 | 0,8 |
| 59 | 3 | 2 | 1 | 4 | 3 | 1 | 3 | 1 | 2 | 2 | 22 | 2,2 | 1,1 | 1 |
| 60 | 3 | 1 | 2 | 5 | 2 | 1 | 4 | 4 | 2 | 1 | 25 | 2,5 | 2,1 | 1,4 |
| 61 | 3 | 2 | 3 | 5 | 2 | 1 | 4 | 5 | 4 | 4 | 33 | 3,3 | 1,8 | 1,3 |
| 62 | 3 | 2 | 2 | 5 | 2 | 1 | 3 | 5 | 3 | 3 | 29 | 2,9 | 1,7 | 1,2 |
| 63 | 2 | 2 | 1 | 3 | 2 | 1 | 3 | 4 | 3 | 3 | 24 | 2,4 | 0,9 | 0,9 |
| 64 | 3 | 3 | 2 | 3 | 2 | 1 | 3 | 4 | 2 | 2 | 25 | 2,5 | 0,7 | 0,8 |
| 65 | 3 | 3 | 1 | 5 | 3 | 1 | 3 | 2 | 3 | 3 | 27 | 2,7 | 1,3 | 1,1 |
| 66 | 4 | 2 | 2 | 2 | 2 | 1 | 3 | 2 | 1 | 1 | 20 | 2,0 | 0,9 | 0,9 |
| 67 | 4 | 2 | 1 | 1 | 2 | 1 | 3 | 2 | 2 | 2 | 20 | 2,0 | 0,9 | 0,9 |
| 68 | 3 | 1 | 3 | 2 | 2 | 1 | 3 | 3 | 4 | 3 | 25 | 2,5 | 0,9 | 0,9 |
| 69 | 2 | 1 | 1 | 2 | 2 | 1 | 3 | 2 | 3 | 3 | 20 | 2,0 | 0,7 | 0,8 |
| Total | 168 | 180 | 173 | 216 | 159 | 121 | 177 | 170 | 155 | 153 | 1672 | 167,2 | 582 | 23 |

11,1 * 0,86 0,96

## ANEXO F. Anexo A. Tabla A.1. Objetivos de control y controles de la norma ISO/IEC 27001:2005

| | | |
|---|---|---|
| **A.5 Política de seguridad** | | |
| **A.5.1 Política de seguridad de la información**<br>Objetivo: Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes. | | |
| A.5.1.1 | Documento de la política de seguridad de la información | Control Un documento de política de seguridad de información será aprobado por la dirección, publicado y comunicado a todos los empleados y partes externas pertinentes |
| A.5.1.2 | Revisión de la política de seguridad de la información | Control La política de seguridad de la información debe revisarse a intervalos planificados o si ocurre cambios significativos asegurar su conveniencia, adecuación y eficacia continua |
| **A.6 Organización de la seguridad de la información** | | |
| **A.6.1 Organización interna**<br>Objetivo: Gestionar la seguridad de la información dentro de la organización. | | |
| A.6.1.1 | Compromiso de la dirección para la seguridad de la información | Control La dirección debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información. |
| A.6.1.2 | Coordinación de la seguridad de información | Control Las actividades de seguridad de la información deben coordinarse con representantes de las diferentes partes de la organización con roles y funciones de trabajo pertinentes. |
| A.6.1.3 | Asignación de responsabilidades de la seguridad de la información | Control Deben definirse claramente las responsabilidades de la seguridad de la información. |
| A.6.1.4 | Proceso de autorización para los recursos de procesamiento de la información | Control: Deben definirse e implementar un proceso de autorización para cada nuevo recurso de procesamiento de la información. |
| A.6.1.5 | Acuerdos de confidencialidad | Control be identificarse y revisarse regularmente los requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información. |
| A.6.1.6 | Contacto con las autoridades | Control Deben mantenerse los contactos apropiados con las autoridades pertinentes. |
| A.6.1.7 | Contacto con grupos interesados especiales | Control Deben mantenerse los contactos apropiados con grupos de interés especial u otros foros de especialistas de seguridad y asociaciones profesionales. |

| | | |
|---|---|---|
| A.6.1.8 | Revisión independiente de la seguridad de la información | Control<br>El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad. |
| **A.6.2 Entidades externas**<br>Objetivo: Mantener la seguridad de la información y recursos de procesamiento de información de la organización que son accesados, procesados, comunicados o gestionados manejados por partes externas. | | |
| A.6.2.1 | Identificación de riesgos relacionados a partes externas | Control<br>Los riesgos a la información y recursos de procesamiento de la información de la organización para los procesos del negocio que involucran partes externas deben identificarse y deben implementarse los controles apropiados antes de otorgar el acceso. |
| A.6.2.2 | Tratamiento de la seguridad en las relaciones con clientes | Control<br>Todos los requisitos de seguridad identificados deben tratarse antes de dar acceso a los clientes a la información o activos de la organización. |
| A.6.2.3 | Tratamiento de la seguridad en los acuerdos de terceras partes. | Control Los acuerdos con usuarios de terceras partes que involucran acceder, procesar, comunicar o gestionar la información de la organización o los recursos para el tratamiento de la información, o agregar productos o servicios a recursos para el tratamiento de la información deben cubrir todos requisitos de seguridad pertinentes. |
| **A.7 Gestión de activos** | | |
| **A.7.1 Responsabilidad por los activos**<br>Objetivo: Alcanzar y mantener la protección apropiada de los activos de la organización. | | |
| A.7.1.1 | Inventario de activos | Control: Todos los activos deben identificarse claramente y elaborarse y mantenerse el inventario de todos los activos importantes. |
| A.7.1.2 | Propiedad de los activos | Control Toda información y activos asociados con las instalaciones de procesamiento de la información deben ser “dueños” por una parte designada de la organización |
| A.7.1.3 | Utilización aceptable de los activos | Control Deben identificarse, documentarse e implementarse las reglas para la utilización aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información |

| | | |
|---|---|---|
| **A.7.2. Clasificación de la información**<br>Objetivo: asegurar que la información reciba un nivel apropiado de protección | | |
| A.7.2.1 | Directrices de clasificación | Control La información debe clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la organización. |
| A.7.2.2 | Etiquetado y manejo de la información | Control Un conjunto apropiado de procedimientos para etiquetar y manejar la información debe desarrollarse e implementarse de acuerdo con el esquema de clasificación adoptado por la organización. |
| **A.8 Seguridad de recursos humanos** | | |
| **A.8.1. Antes del empleo**<br>Objetivo: Asegurar que los empleados, los contratistas y usuarios de terceras partes comprendan sus responsabilidades, y que sean apropiados para los roles considerados, y para reducir el riesgo del robo, fraude o mal uso de los recursos. | | |
| A.8.1.1 | Roles y responsabilidades | Control Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios terceras partes deben definirse y documentarse de acuerdo con la política de seguridad de la información de la organización. |
| A.8.1.2 | Selección | Control La verificación de los antecedentes sobre todos los candidatos para empleados, contratistas y usuarios de terceras partes deben llevarse a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y proporcionarles a los requisitos del negocio, a la clasificación de la información acezada, y los riesgos percibidos. |
| A.8.1.3 | Términos y condiciones de empleo | Control Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben acordar y firmar los términos y condiciones de su contrato, que debe declarar sus responsabilidades por la seguridad de la información de la organización. |

| | | |
|---|---|---|
| **A.8.2 Durante el empleo**<br>Objetivo: Asegurar que todos los empleados, contratistas y usuarios de terceras partes son conscientes de las amenazas, y aspectos relacionados con la seguridad de la información, sus responsabilidades y obligaciones, y que estén equipadas para respaldar la política de seguridad de la organización en el curso normal de su trabajo, y reducir el riesgo de error humano. | | |
| A.8.2.1 | Responsabilidades de la dirección | Control La dirección debe requerir que los empleados, contratistas y usuarios de terceras apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos de la organización. |

| | | |
|---|---|---|
| A.8.2.2 | Toma de conciencia, educación y formación en la seguridad de la información | Control Todos los empleados de la organización y, cuando sean pertinentes los contratistas y usuarios de terceras partes deben recibir la formación en toma de conciencia y las actualizaciones regulares apropiadas en las políticas y procedimientos de la organización como sea pertinente para su función de trabajo. |
| A.8.2.3 | Proceso disciplinario | Control Debe haber un proceso disciplinario formal para los empleados quienes cometan un incumplimiento |
| **A.8.3 Terminación o cambio de empleo**<br>Objetivo: Asegurar que los empleados, contratistas y usuarios de terceras partes se retiran de una organización o cambian el empleo de una manera ordenada. | | |
| A.8.3.1 | Responsabilidades de la terminación | Control Debe definirse y asignarse claramente las responsabilidades para llevar a cabo la terminación o cambio de empleo. |
| A.8.3.2 | Devolución de los activos | Control Todos los empleados, contratistas y usuarios de terceras partes deben devolver todos los activos de la organización en su posesión una vez terminado su empleo, contrato o acuerdo. |
| A.8.3.3 | Retiro de los derechos de acceso | Control Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes a la información y recursos para el procesamiento de la información deben retirarse una vez terminado su empleo, contrato o acuerdo, o una vez ajustado el cambio. |
| **A.9 Seguridad física y ambiental** | | |
| **A.9.1 Áreas seguras**<br>Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones e información de la organización | | |
| A.9.1.1 | Perímetro de seguridad física | Control: Los perímetros de seguridad (barreras tales como paredes, puertas de entradas controladas por tarjeta, o puesto de recepción manual) deben utilizarse para proteger las áreas que contienen la información y las instalaciones de procesamiento de la información. |
| A.9.1.2 | Controles físicos de entrada | Control<br>Las áreas de seguridad deben estar protegidas por controles de entrada apropiados que aseguren el permiso de acceso sólo al personal autorizado. |
| A.9.1.3 | Seguridad de oficinas, habitaciones e instalaciones | Control Debe diseñarse y aplicarse la seguridad física para oficinas, habitaciones e instalaciones. |
| A.9.1.4 | Protección contra las amenazas externas y ambientales | Control Debe diseñarse y aplicarse la protección física contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastres natural o hecho por el hombre. |

| | | |
|---|---|---|
| A.9.1.5 | Trabajo en áreas seguras | Control: Debe diseñarse y aplicarse la protección física y las directrices para trabajar en áreas seguras. |
| A.9.1.6 | Áreas de acceso al público, entrega y carga | Control Los puntos accesos como las áreas de entrega y carga y otras donde las personas no autorizadas pueden entrar en las instalaciones deben controlarse y, si es posible, aislarse de instalaciones de procesamiento de la información para evitar el acceso no autorizado. |
| **A.9.2 Seguridad de los equipos**<br>Objetivo: Prevenir pérdidas, daños, robo o comprometer los activos e interrupción de las actividades de la organización. | | |
| A.9.2.1 | Ubicación y protección del equipo | Control El equipo debe ubicarse o protegerse para reducir los riesgos de amenazas y peligros ambientales, y oportunidades para el acceso no autorizado. |
| A.9.2.2 | Servicio de apoyo | Control El equipo debe protegerse contra fallas de energía y otras interrupciones eléctricas causadas por fallas en los servicios de apoyo. |
| A.9.2.3 | Seguridad del cableado | Control El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe protegerse contra intercepción o daño. |
| A.9.2.4. | Mantenimiento de equipos | Control Los equipos deben mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. |
| A.9.2.5. | Seguridad de equipos fuera de las instalaciones de la organización. | Control: Debe aplicarse la seguridad a los equipos exteriores teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. |
| A.9.2.6 | Seguridad en la reutilización o eliminación de equipos | Control Todos los elementos del equipo que contengan dispositivos de almacenamiento de datos deben controlarse para asegurar que cualquier dato sensible y software bajo licencia ha sido removido o tachado antes de su disposición. |
| A.9.2.7 | Retiro de la propiedad | Control No deben sacarse de las instalaciones sin autorización, los equipos, la información o el software. |
| **A.10 Gestión de comunicaciones y operaciones** | | |
| **A.10.1 Procedimiento y responsabilidades de operación**<br>Objetivo: Asegurar la operación correcta y segura de los recursos de tratamiento de información | | |
| A.10.1.1 | Documentación de procedimientos operativos | Control Los procedimientos operativos deben documentarse, mantenerse, y estar disponibles a todos usuarios que los necesitan. |

| | | |
|---|---|---|
| A.10.1.2 | Gestión de cambio | Control Deben controlarse los cambios para los recursos y sistemas de procesamiento de la información |
| A.10.1.3 | Segregación de tareas | Control Las tareas o áreas de responsabilidad deben segregarse para reducir las oportunidades de modificación no autorizadas o uso de los activos de la organización |
| A.10.1.4 | Separación de los recursos para el desarrollo, prueba/ensayo y operación | Control Deben separarse los recursos para el desarrollo, prueba/ensayo y operación para reducir los riesgos de acceso no autorizado o cambios al sistema operativo. |
| **A.10.2. Gestión de entrega de servicio de tercera parte**<br>Objetivo: implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicio de tercera parte | | |
| A.10.2.1 | Entrega del servicio | Control. Debe asegurarse que los controles de seguridad, las definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio de tercera parte son implementados, operados y mantenidos por la tercera parte. |
| A.10.2.2 | Seguimiento y revisión de los servicios de tercera parte | Control los servicios, informes y registros suministrados por la tercera parte deben ser seguidos y revisados regularmente y deben ser llevadas a cabo auditorias regularmente. |

| | | |
|---|---|---|
| A.10.2.3 | Gestión de cambios para los servicios de tercera parte | Control Los cambios para el suministro de servicios, incluyendo el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de información existentes, deben gestionarse, tomando en cuenta la criticidad del sistema del negocio y los procesos involucrados y la re-evaluación de los riesgos. |
| **A.10.3 Planificación y aceptación del sistema**<br>Objetivo: Minimizar el riesgo de fallas de los sistemas | | |
| A.10.3.1 | Gestión de capacidad | Control Debe realizarse seguimiento, ajustes y proyecciones de los requisitos de la capacidad futura de la utilización de los recursos, para asegurar el desempeño del sistema requerido. |
| A.10.3.2 | Aceptación del sistema | Control Deben establecerse los criterios de aceptación para los nuevos sistemas de información y versiones nuevas o mejoradas y deben desarrollarse pruebas adecuadas de los sistemas durante el desarrollo y antes de la aceptación. |

| | | |
|---|---|---|
| **A.10.4 Protección contra código malicioso y movible**<br>Objetivo: Proteger la integridad del software y de la información | | |
| A.10.4.1 | Controles contra código malicioso | Control Deben implantase los controles de detección, prevención y recuperación para la protección contra código maliciosos, y procedimientos adecuados de toma de conciencia de los usuarios. |
| A.10.4.2 | Control contra código movible | Control Donde la utilización de código movible esta autorizada, la configuración debe asegurar que el código movible autorizado opera de acuerdo a una política de seguridad claramente definida, y debe prevenirse el ejecutar el código movible no autorizado |
| **A.10.5 Copia de seguridad**<br>Objetivo: Mantener la integridad y la disponibilidad y los recursos de procesamiento de la información | | |
| A.10.5.1 | Copia de seguridad de la información | Control: Las copias de seguridad de la información y software deben ser tomadas y probadas con regularidad de acuerdo con la política de copia de seguridad acordada |

| | | |
|---|---|---|
| **A.10.6 Gestión de seguridad de la red**<br>Objetivo: Asegurar la protección de la información en las redes y la protección de su infraestructura de soporte. | | |
| A.10.6.1 | Controles de red | Control Las redes deben gestionarse y controlarse adecuadamente, a fin de estar protegidas de las amenazas, y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la información en tránsito. |
| A.10.6.2 | Seguridad de servicios de red. | Control Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red deben identificarse e incluirse en cualquier acuerdo de servicio de red, ya sea que estos servicios sean proporcionados en la empresa o subcontratados. |
| **A.10.7 Manejo de medios de información**<br>Objetivo: Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de los activos, e interrupción de las actividades del negocio. | | |
| A.10.7.1 | Gestión de medios movibles | Control Deben existir procedimientos para la gestión de medios removibles. |
| A.10.7.2 | Disposición de medios | Control<br>Cuando ya no son requeridos los medios de información deben eliminarse de forma segura y sin peligro, utilizando procedimientos formales. |

| | | |
|---|---|---|
| A.10.7.3 | Procedimientos de manejo de la información | Control: Se deben establecer procedimientos para el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada. |
| A.10.7.4 | Seguridad de la documentación de sistema | Control La documentación de sistema debería protegerse contra el acceso no autorizado |
| **A.10.8 Intercambio de información**<br>Objetivo: Mantener la seguridad de la información y el software intercambiado dentro de una organización y con cualquier entidad externa | | |
| A.10.8.1 | Políticas y procedimientos de intercambio de información | Control Deben establecerse políticas, procedimientos de intercambio formales, y controles para proteger el intercambio de información a través de la utilización de toda clase de recursos de comunicación. |
| A.10.8.2 | Acuerdo de intercambio | Control Deben establecerse acuerdos, para el intercambio de información y software entre la organización y partes externas. |
| A.10.8.3 | Medios de información físicos en tránsito | Control Los medios que contienen la información deben protegerse contra el acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización. |
| A.10.8.4 | Mensaje electrónico | Control Debe estar apropiadamente protegida la información involucrada en el mensaje electrónico. |
| A.10.8.5 | Sistema de información del negocio | Control Deben desarrollarse e implementarse las políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio. |
| **A.10.9 Servicios de comercio electrónico**<br>Objetivo: Asegurar la seguridad de servicios de comercio electrónico, y su utilización segura | | |
| A.10.9.1 | Comercio electrónico | Control La información involucrada en la transferencia de comercio electrónico en redes públicas debe protegerse de la actividad fraudulenta, litigios contractuales, y la divulgación o modificación no autorizada. |
| A.10.9.2 | Transacciones en línea | Control La información involucrada en las transacciones en línea debe protegerse para prevenir la transmisión incompleta, perdida de ruta, alteración de mensaje no autorizado, divulgación no autorizada y duplicación o repetición de mensaje no autorizada |
| A.10.9.3 | Información disponible públicamente | Control La integridad de la información que esta disponible sobre un sistema disponible públicamente debe protegerse para prevenir la modificación no autorizada. |

| | | |
|---|---|---|
| **A.10.10 Seguimiento**<br>Objetivo: Detectar las actividades de procesamiento de la información no autorizada. | | |
| A.10.10.1 | Registro de auditoria | Control Deben producirse y mantenerse los registros de auditorias que registren actividades, excepciones y eventos de seguridad de la información del usuario, durante un periodo definido para ayudar en futuras investigaciones y seguimiento del control de accesos. |
| A.10.10.2 | Seguimiento de la utilización de los sistemas | Control: Deben establecerse los procedimientos para el seguimiento de la utilización de los recursos de procesamiento de la información y los resultados de las actividades de seguimiento revisadas regularmente. |
| A.10.10.3 | Protección de la información de registro | Control Deben protegerse los recursos de registro e información de registro contra el acceso manipulado y no autorizado |
| A.10.10.4 | Administrador y operador de registros | Control Deben registrase las actividades del administrador del sistema y el operador del sistema. |
| A.10.10.5 | Registro de fallas | Control<br>Las fallas deben registrase, analizarse y tomarse las acciones apropiadas |
| A.10.10.6 | Sincronización de relojes | Control Los relojes de todos los sistemas de procesamiento de la información pertinentes dentro de una organización o dominio de seguridad deben sincronizarse con una fuente de tiempo exacta acordada. |
| **A.11 Control de accesos** | | |
| **A.11.1 Requisitos del negocio para el control de accesos**<br>Objetivo: Controlar los accesos a la información | | |
| A.11.1.1 | Política de control de accesos | Control Debe establecerse, documentarse y revisarse una política de control de accesos, basado en los requisitos del negocio y de seguridad para el acceso. |
| **A.11.2 Gestión de accesos de usuarios**<br>Objetivo: Asegurar el accesos del usuarios autorizado y prevenir el acceso no autorizado a los sistemas de información | | |
| A.11.2.1 | Registro de usuarios | Control. Debe existir un procedimiento formal de registro y des-registro de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información. |
| A.11.2.2 | Gestión de privilegios | Control Deben restringirse y controlarse la utilización y asignación de privilegios |
| A.11.2.3 | Gestión de contraseñas de usuarios | Control: Debe controlarse la asignación de contraseñas a través de un proceso de gestión formal. |

| | | |
|---|---|---|
| A.11.2.4 | Revisión de los derechos de acceso de usuario | Control: La dirección debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal. |
| **A.11.3 Responsabilidades de usuarios**<br>Objetivo: Prevenir el acceso de usuarios no autorizados, y comprometer o robar la información y los recursos de procesamiento de información | | |
| A.11.3.1 | Uso de contraseñas | Control: Debe requerirse a los usuarios seguir las buenas prácticas de seguridad para la selección y uso de sus contraseñas. |
| A.11.3.2 | Equipo desatendidos | Control Los usuarios deben asegurarse que los equipos desatendidos estén debidamente protegidos. |
| A.11.3.3 | Políticas de escritorios y pantallas limpias. | Control Para los recursos de procesamiento de información, debe adoptarse una política de escritorios limpios de papel y de dispositivos de almacenamientos removibles y una política de pantallas limpias. |
| **A.11.4 Control de acceso a la red**<br>Objetivo: Prevenir el acceso no autorizado a los servicios de red | | |
| A.11.4.1 | Política de utilización de los servicios de red | Control. Los usuarios sólo deben tener acceso a los servicios que han sido específicamente autorizados a utilizar. |
| A.11.4.2 | Autenticación de usuarios para conexiones externas | Control. Deben utilizarse métodos de autenticación apropiados para controlar el acceso por usuarios remotos. |
| A.11.4.3 | Identificación de equipos en redes | Control. Debe considerarse ala identificación de equipo automático como un medio de autentificar las conexiones de ubicaciones y equipos específicos. |
| A.11.4.4 | Protección del diagnóstico remoto y de la configuración de puerto | Control. Debe controlarse el acceso físico y lógico para el diagnóstico y configuración de los puertos. |
| A.11.4.5 | Segregación en redes | Control: Deben segregarse los grupos de los servicios de información, los usuarios, y los sistemas de información en redes. |
| A.11.4.6 | Control de conexión de redes | Control Para redes compartidas, especialmente aquellas que atraviesas las fronteras de la organización, la capacidad de usuarios a conectarse a la red deben restringirse, de acuerdo con la política de control de acceso y los requisitos de las aplicaciones del negocio (véase apartado 11.1) |
| A.11.4.7 | Control de direccionamiento en la red | Control: Deben implementarse los controles de direccionamiento a redes para asegurar que las conexiones entre computadoras y los flujos de información no violen la política de control de accesos de las aplicaciones del negocio. |

| | | |
|---|---|---|
| **A.11.5 Control de acceso al sistema operativo**<br>Objetivo: Prevenir el acceso no autorizado a los sistemas operativos | | |
| A.11.5.1 | Procedimientos de conexión segura | Control: Debe controlarse el acceso a los sistemas operativos por un procedimiento de conexión segura. |
| A.11.5.2 | Identificación y autenticación del usuario. | Control<br>Todos los usuarios deben disponer de un identificador único (ID de usuario) sólo para su uso personal y debe seleccionarse una técnica de autenticación adecuada, para probar la identidad declarada de un usuario. |
| A.11.5.3 | Sistema de gestión de contraseña | Control Los sistemas para la gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. |
| A.11.5.4 | Utilización de las prestaciones del sistema. | Control Debe restringirse y controlarse estrechamente la utilización de programas de servicio que podrían ser capaces de eludir las medidas de control del sistema y de las aplicaciones. |
| A.11.5.5 | Sesión inactiva | Control Las sesiones inactivas deben apagarse después de un período definido de la inactividad. |
| A.11.5.6 | Limitación del tiempo de conexión | Control Las restricciones al horario deben ser utilizadas para proporcionar seguridad adicional a las aplicaciones de alto riesgo. |
| **A.11.6 Control de acceso a las aplicaciones e información**<br>Objetivo: Prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación | | |
| A.11.6.1 | Restricción de acceso a la información | Control El acceso a la información y a las funciones del sistema de aplicación por usuarios y personal de soporte debe restringirse de acuerdo con la política de control de acceso definida. |
| A.11.6.2 | Aislamiento de sistemas sensibles. | Control Los sistemas sensibles deben tener un entorno informático dedicado (aislados) |
| **A.11.7 Computación móvil y trabajo a distancia**<br>Objetivo: Asegurar la seguridad de la información cuando se utilizan recursos de computación móvil y de trabajo a distancia. | | |
| A.11.7.1 | Computación móvil y comunicaciones | Debe implantarse una política formal, y deben adoptarse las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar recursos de computación móvil |
| A.11.7.2 | Trabajo a distancia | Control: Deben desarrollarse e implementarse políticas, planes operacionales y procedimientos para las actividades de trabajo a distancia. |

| | | |
|---|---|---|
| **A.12 Adquisición, desarrollo y mantenimiento de sistemas de información** | | |
| **A.12.1 Requisitos de seguridad de los sistemas de información**<br>Objetivo: Asegurar que la seguridad es una parte integral de los sistemas de información | | |
| A.12.1 | Análisis y especificación de los requisitos de seguridad | Control Las declaraciones de los requisitos del negocio para los nuevos sistemas de información o mejoras a los sistemas de información existentes deben especificar los requisitos de control de seguridad. |
| **A.12.2 Procesamiento correcto en las aplicaciones**<br>Objetivo: Prevenir los errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones. | | |
| A.12.2.1 | Validación de los datos de entrada | Control Deben validarse los datos de entrada a las aplicaciones para asegurarse de que éstos son correctos y apropiados |
| A.12.2.2 | Control del procesamiento interno | Deben incorporarse a las aplicaciones las comprobaciones de validación para detectar cualquier corrupción de la información a través de los errores de procesamiento o actos deliberados |
| A.12.2.3 | Integridad de mensaje | Control<br>Deben identificarse los requisitos para asegurar la autenticidad y proteger la integridad de mensajes en aplicaciones e identificarse e implementarse los controles apropiados. |
| A.12.2.4 | Validación de los datos de salida | Control Deben validarse los datos de salida de una aplicación para asegurarse de que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias. |
| **A.12.3. Controles criptográficos**<br>Objetivos: Proteger la confidencialidad, autenticidad o integridad de la información por los medios criptográficos | | |
| A.12.3.1 | Políticas sobre la utilización de controles criptográficos | Control Debe desarrollarse e implementarse una política sobre la utilización de controles criptográficos para la protección de la información |
| A.12.3.2 | Gestión de claves | Control Debe establecerse la gestión de clave para dar apoyo a la utilización por la organización de técnicas criptográficas. |
| **A.12.4. Seguridad de los archivos del sistema**<br>Objetivo: Asegurar la seguridad de los archivos del sistema | | |
| A.12.4.1 | Control del software operativo | Control: Deben existir procedimientos establecidos para controlar la instalación del software en sistemas en funcionamiento |
| A.12.4.2 | Protección de los datos de prueba del sistema | Control Deben seleccionarse cuidadosamente y protegerse y controlarse los datos de prueba |

| | | |
|---|---|---|
| A.12.4.3 | Control de acceso al código fuente del programa | Control Debe restringirse el acceso al código fuente del programa |
| **A.12.5 Seguridad en los procesos de desarrollo y soporte**<br>Objetivo: Mantener la seguridad del software y la información del sistema de aplicación | | |
| A.12.5.1 | Procedimientos de control de cambios | Control La implementación de los cambios debe ser controlada por la utilización de procedimientos formales de control de cambio. |
| A.12.5.2 | Revisión técnica de aplicaciones después de los cambios de sistemas operativos | Control. Cuando los sistemas operativos son cambiados, deben revisarse y probarse las aplicaciones críticas del negocio para asegurar de que no hay impacto adverso sobre las operaciones o la seguridad de la organización. |
| A.12.5.3 | Restricciones en los cambios a los paquetes de software | Control: Las modificaciones a paquetes de software deben ser desalentadas, limitadas a los cambios necesarios, y todo cambio debe controlarse estrictamente. |
| A.12.5.4 | Fuga de información | Control Deben prevenirse las oportunidades de fuga de información |
| A.12.5.5 | Desarrollo de software contratado externamente. | Control. La organización debe supervisar y realizar seguimiento al desarrollo de software contratado externamente. |
| **A.12.6 Gestión de vulnerabilidad técnica**<br>Objetivo: Reducir los riesgos que resultan de la explotación de las vulnerabilidades técnicas publicadas | | |
| A.12.6.1 | Control de las vulnerabilidades técnicas | Control. Debe obtenerse la información oportuna sobre las vulnerabilidades técnicas del sistema de información que ésta siendo utilizado, evaluarse la exposición de la organización a tales vulnerabilidades y tomarse las medidas apropiadas para tratar el riesgo asociado. |
| **A.13 Gestión de incidente de seguridad de la información** | | |
| **A.13.1 Reportar los eventos y debilidades de seguridad de la información**<br>Objetivo: Asegurar que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente. | | |
| A.13.1.1 | Reporte de los eventos de seguridad de la información | Control deben reportase los eventos de seguridad de la información a través de los canales de gestión apropiados tan rápidamente como sea posible. |
| A.13.1.2 | Reporte de debilidades de seguridad | Control. Debe requerirse a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información, detectar e informar cualquier debilidad en la seguridad de los sistemas o servicios, que haya sido observada o sospechada. |
| **A.13.2 Gestión de los incidentes y mejoras de seguridad de la información** | | |

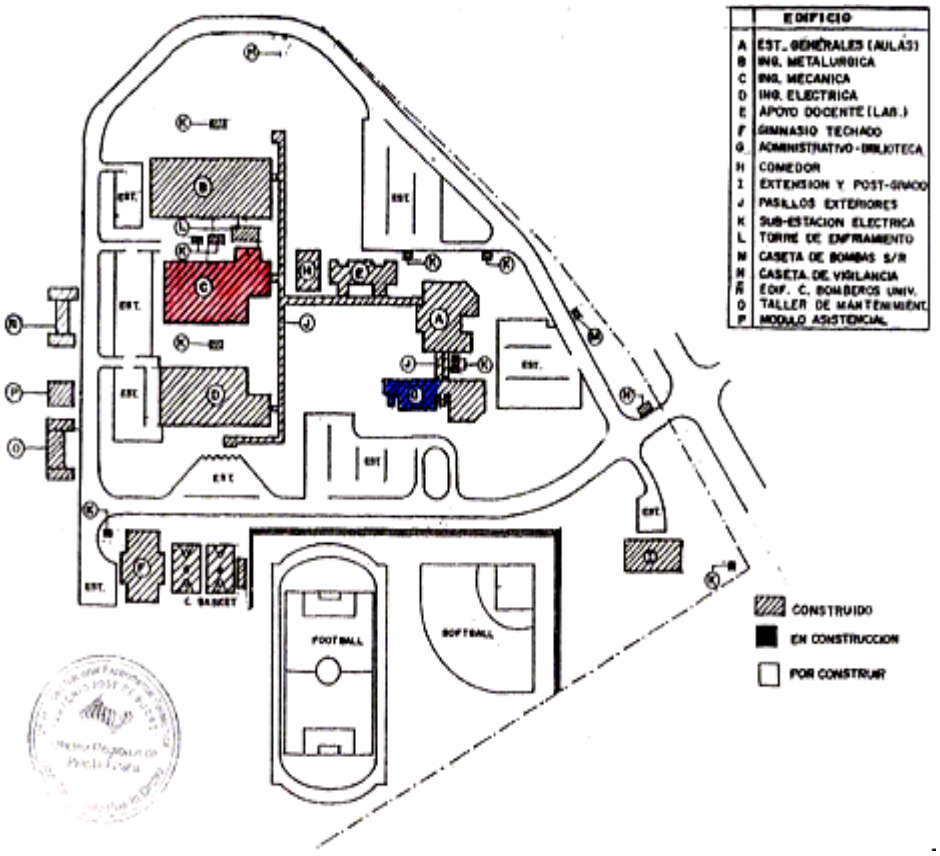
| | | |
|---|---|---|
| Objetivo: Asegurar que un enfoque coherente y eficaz es aplicado a la gestión de los incidentes de seguridad de la información | | |
| A.13.2.1 | Responsabilidades y procedimientos | Control Deben establecerse las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información. |
| A.13.2.2 | Aprendizaje de los incidentes de seguridad de la información | Control Deben establecerse mecanismos que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de seguridad de información |
| A.13.2.3 | Recolección de evidencias | Control: Cuando una acción de seguimiento contra una persona u organización, después de un incidente de seguridad de la información que involucra acciones legales (civiles o criminales), deben recolectarse, conservarse y presentarse evidencias conforme a las reglas establecidas por la legislación aplicable o por el tribunal que sigue el caso. |
| **A.14 Gestión de continuidad del negocio** | | |
| **A.14.1 Aspectos de seguridad de la información de la gestión de continuidad del negocio**<br>Objetivo: Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas significativas o desastres de los sistemas de información y asegurar su reanudación oportuna | | |
| A.14.1.1 | Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio | Control. Un proceso dirigido debe ser desarrollado mantenido para la continuidad del negocio a través de la organización que trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. |
| A.14.1.2 | Continuidad del negocio y evaluación de riesgo | Control. Los eventos que pueden causar las interrupciones a los procesos del negocio deben identificarse, al mismo tiempo que la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información. |
| A.14.1.3 | Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información | Control Deben desarrollarse e implementarse planes para mantener y recuperar las operaciones y asegurar la disponibilidad de la información al nivel requerido y en los plazos requeridos, tras la interrupción o la falla de los procesos críticos del negocio. |
| A.14.1.4 | Marco de planificación para la continuidad del negocio | Control: Se debe mantener un esquema único de planes de continuidad del negocio para asegurar que dichos planes son coherentes, para tratar los requisitos de seguridad de la información y para identificar las prioridades de prueba y mantenimiento |
| A.14.1.5 | Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio | Control: Deben probarse y actualizarse con regularidad los planes de continuidad del negocio para asegurarse de su actualización y eficacia. |

| | | |
|---|---|---|
| **A.15 Cumplimiento** | | |
| **A.15.1 Cumplimiento de requisitos legales**<br>Objetivo: Evitar incumplimientos de cualquier ley, estatuto, obligación reglamentarias o contractuales, y de cualquier requisito de seguridad | | |
| A.15.1.1 | Identificación de la legislación aplicable | Control. Deben definirse, documentarse y mantenerse actualizados todos los requisitos legales, reglamentarios y contractuales pertinentes y el enfoque de la organización que cumplan estos requisitos para cada sistema de información y de la organización. |
| A.15.1.2 | Derecho de la propiedad intelectual (DPI) | Control Deben implementarse los procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material protegido por derechos de propiedad intelectual, y sobre el uso de productos de software reservados. |
| A.15.1.3 | Protección de los registros de la organización | Control. Deben protegerse los registros importantes contra la pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales y del negocio. |
| A.15.1.4 | Protección de datos y de la privacidad de la información personal | Control Deben asegurarse la protección de datos y la privacidad como sea requerido en la legislación, las reglamentaciones pertinentes, y si es aplicable, en las cláusulas contractuales. |
| A.15.1.5 | Prevención del mal uso de los recursos de procesamiento de la información. | Control<br>Debe disuadirse a los usuarios de utilizar los recursos de procesamiento de la información para propósitos no autorizados. |
| A.15.1.6 | Regulación de controles criptográficos | Control<br>Deben utilizarse los controles criptográficos en cumplimiento con todos los acuerdos, leyes y regulaciones pertinentes. |
| **A.15.2 Cumplimiento con las políticas y normas de seguridad y el cumplimiento técnico**<br>Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad de la organización | | |
| A.15.2.1 | Cumplimiento con las políticas y normas de seguridad | Control:<br>Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad son llevados a cabo correctamente para alcanzar el cumplimiento con las normas y políticas de seguridad. |
| A.15.2.2 | Comprobación del cumplimiento técnico | Control<br>Debe comprobarse regularmente la compatibilidad de los sistemas de información con las normas de implementación de seguridad |

| **A.15.3 Consideraciones de auditoria de los sistemas de información**<br>Objetivo: Maximizar la efectividad y minimizar las interferencias en el proceso de auditoria del sistema de la información. | | |
|---|---|---|
| A.15.3.1 | Controles de auditoria de los sistemas de información | Control<br>Deben planificarse cuidadosamente y acordarse los requisitos y actividades de auditoria que involucren comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio |
| A.15.3.2 | Protección de las herramientas de auditoria de los sistemas de información | Control<br>Debe protegerse el acceso a las herramientas de auditoria del sistema de la información para prevenir cualquier posible mal uso o compromiso |

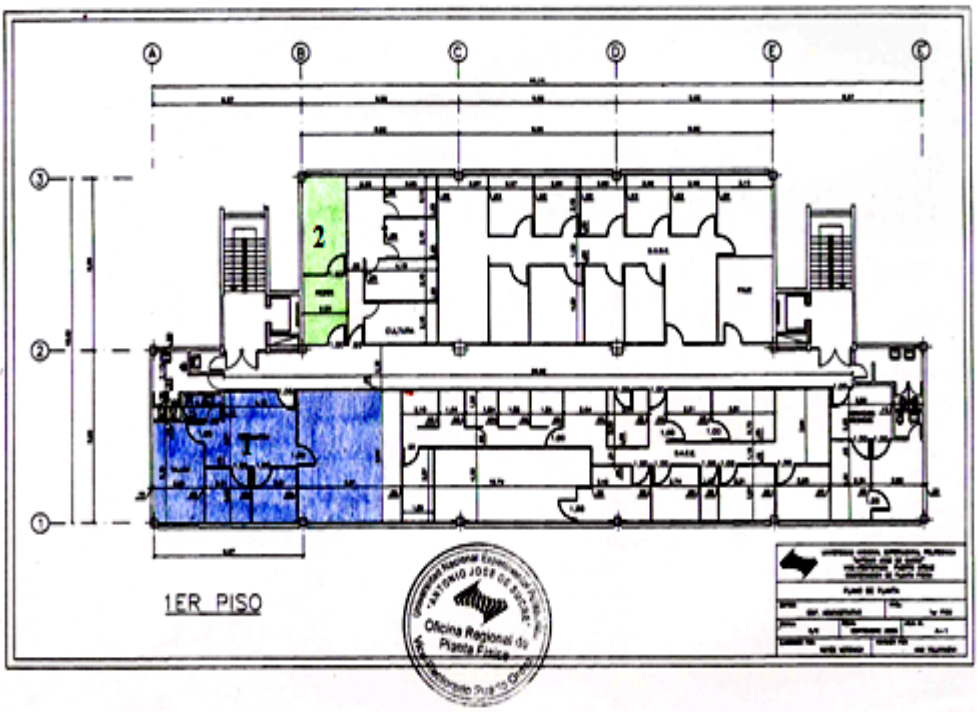
## ANEXO G. MICROLOCALIZACIÓN DEL PROYECTO

### Campus UNEXPO – Vicerrectorado de Puerto Ordaz



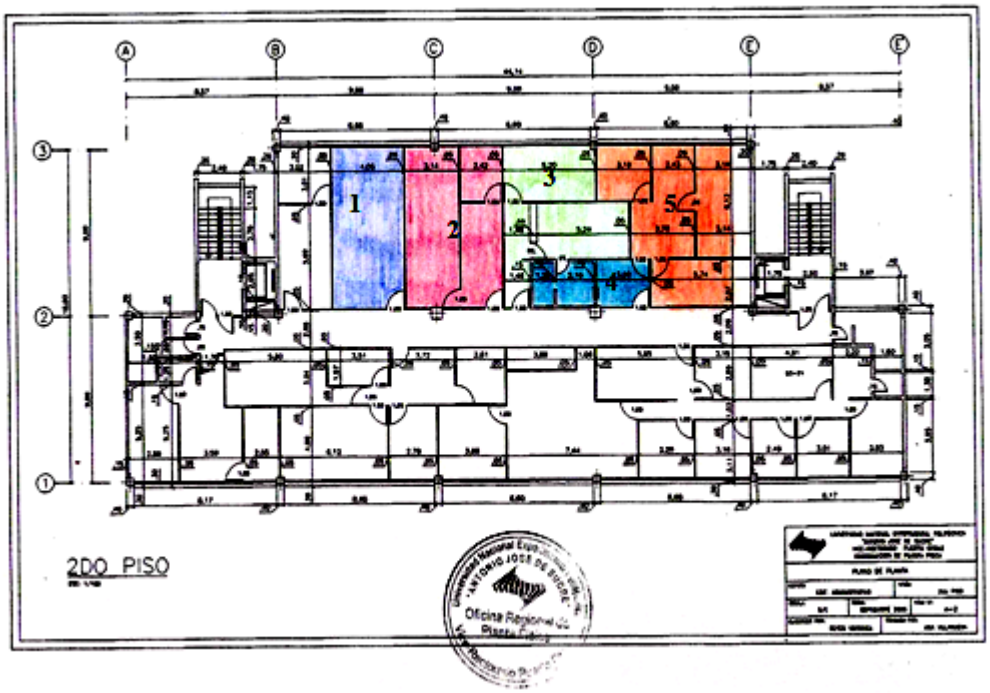

| Leyenda | |
|---|---|
| | Edificio Administrativo |
| | Edificio de Mecánica/Industrial |

### 1er PISO DEL EDIFICIO ADMINISTRATIVO



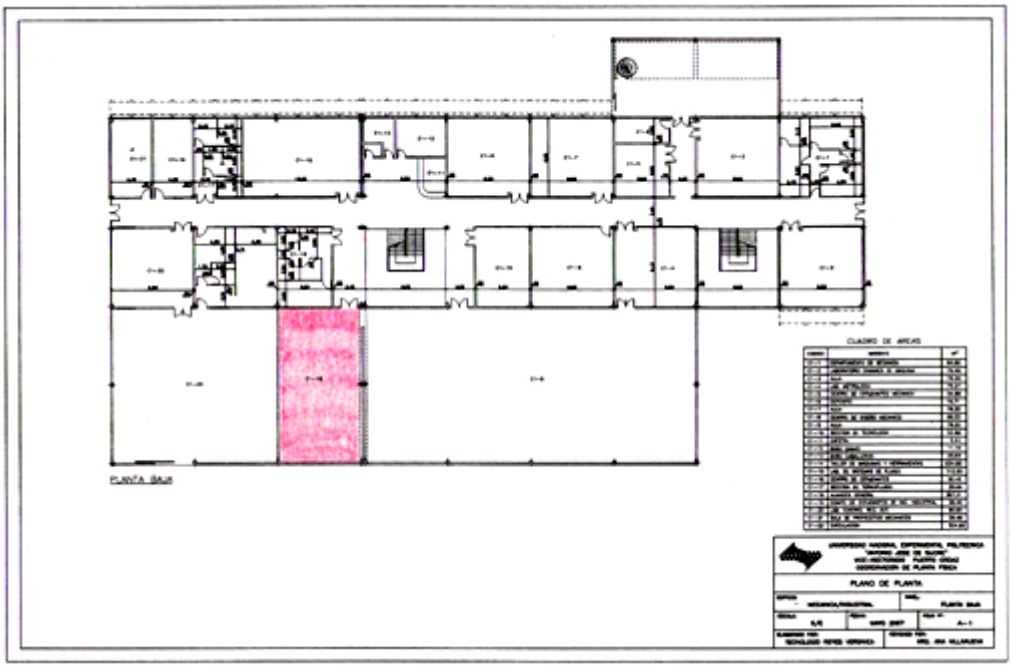

| Leyenda | |
|---|---|
| | 1. Oficina Regional de Tecnología y Servicios de Información |
| | 2. Sala de Cableado principal y de Servidores |

**2do PISO DEL EDIFICIO ADMINISTRATIVO**




| Leyenda | |
|---|---|
| | 1. Oficina Regional de Presupuesto |
| | 2. Oficina Regional de Compra |
| | 3. Unidad de Finanzas |
| | 4. Tesorería |
| | 5. Oficina de Contabilidad |

**PLANTA BAJA DEL EDIFICIO DE INDUSTRIAL/MECÁNICA**



| Leyenda |
| --- |
| Almacén General |

## ANEXO H. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNEXPO

### Alcance de las Políticas

Las políticas definidas en el presente documento aplican a todos los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de la UNEXPO, personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos de la UNEXPO.

### Definiciones

Entiéndase para el presente documento los siguientes términos:

**UNEXPO:** Universidad Nacional Experimental Politécnica "Antonio José de Sucre"

**OCTSI:** Oficina Central de Tecnología y Servicios de Información

**ORTSI:** Oficina Regional de Tecnología y Servicios de Información

**Activo:** Cualquier cosa que tenga valor para la organización. (ISO/IEC 13335-1:2004).

**Ataque cibernético:** intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

**Brecha de seguridad:** deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en si misma, sea o no protegida por reserva legal.

**Certificado Digital:** un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

**Cifrar:** quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama `descodificar" o `descifrar". Los sistemas de ciframiento se llaman "sistemas criptográficos".

**Criptografía de llave publica:** es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

**Información:** Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o

utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

**Integridad:** Propiedad de salvaguardar la exactitud y la totalidad de los activos. (ISO/IEC 13335-1:2004)

**Evento de seguridad de la información:** Una ocurrencia identificada de un estado del sistema, servicio o red que indica una brecha posible en la política de seguridad o falla de la salvaguardas, o de una situación previamente desconocida que puede ser pertinente a la seguridad. (ISO/IEC TR 18044:2004).

**No repudio:** este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

**Política:** son instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.

**Recurso Informático:** Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información adicionalmente pueden involucrase otras propiedades como autenticidad, responsabilidad, no repudio y confiabilidad. (ISO/IEC 17799:2005).

**Usuarios Terceros:** Todas aquellas personas naturales o jurídicas, que no son funcionarios de la UNEXPO, pero que por las actividades que realizan en la Universidad, deban tener acceso a Recursos Informáticos.

## Descripción de las Políticas

### Política 1: Acceso a la Información

1.1. Todos los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO, deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos de la UNEXPO, el Vicerrector Regional, los Jefes de Departamentos o Unidades Administrativas, líder técnico y usuario del proyecto y el responsable del grupo de Seguridad y Control de la ORTSI debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

1.2. El otorgamiento de acceso a la información esta regulado mediante las normas y procedimientos definidos por la OCTSI para tal fin.

1.3. Todas las prerrogativas para el uso de los sistemas de información de la UNEXPO deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Universidad.

1.4. Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

1.5. Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Universidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Universidad.

1.6. Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Universidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos de seguridad de la información que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

**Política 2: Administración de Cambios**

2.1. Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el Comité Técnico de Control de Cambios de la ORTSI responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. La OCTSI tendrá la facultad de aceptar o rechazar la solicitud.

2.2. Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.

2.3. Para la administración de cambios se efectuará el procedimiento correspondiente definido por el OCTSI y aprobado por el Comité Técnico de Control de Cambios, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

2.4. Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

2.5. Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

**Política 3: Seguridad de la Información**

3.1. Los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO, son responsables de la información que manejan y deberán cumplir con los lineamientos de Tecnología y Servicios de Información de la UNEXPO aprobado por el

Consejo Universitario, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

3.2. Los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO no deben suministrar cualquier información de la Universidad a ningún ente externo sin las autorizaciones respectivas.

3.3. Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

3.4. Los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes que laboran para la UNEXPO, deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad, el buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Universidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario público (Administrativo, Docente y Obrero), contratista o pasante deben comprometerse a no utilizar, comercializar o divulgar los productos o a información generada o conocida durante la gestión en la Universidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información esta en la obligación de reportar el hecho al grupo de Seguridad y Control de la ORTSI.

3.5. Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

**Política 4: Seguridad para los Servicios Informáticos**

4.1. El sistema de correo electrónico, grupos de charla y utilidades asociadas de la universidad debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas y pasantes**.**

4.2. La Universidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, el funcionario o contratista autorizará a la entidad para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

4.3. Los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes que laboran para la UNEXPO no deben utilizar versiones escaneadas de Firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico ó cualquier otro tipo de comunicación electrónica haya sido firmada por la persona que la envía.

4.4. La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la universidad. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.

4.5. Los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la universidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet de la OCTSI.

4.6. En cualquier momento que un trabajador publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la Universidad.

4.7. Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la ORTSI, no utilizar el computador y desconectarlo de la red.

4.8. El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de "no repudio".

4.9. El responsable de la Seguridad y Control en conjunto con la ORTSI debe proveer material para recordar regularmente a los empleados, temporales y consultores acerca de sus obligaciones con respecto a la seguridad de los recursos informáticos.

**Política 5: Seguridad En Recursos Informáticos**

5.1. Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

5.1.1. Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

5.1.2. Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre la Administración de usuarios.

5.1.3. Plan de auditoria: Hace referencia a las pistas o registros de los sucesos relativos a la operación.

5.1.4. Las puertas traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.

5.2. El control de acceso a todos los sistemas de computación de la universidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

5.3. Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes que laboran para la UNEXPO son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

5.4. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

5.5. Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.

5.6. Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a el.

5.7. El nivel de superusuario de los sistemas críticos debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema de la ORTSI.

5.8. Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de ciframiento para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

5.9. Antes de que un nuevo sistema se desarrolle o se adquiera, el Consejo Estratégico de Tecnología y Servicios de Información de la UNEXPO, deberán definir las especificaciones y requerimientos de seguridad necesarios.

5.10. La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

5.11. Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

**Política 6: Seguridad en Comunicaciones**

6.1. Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Universidad, deberán ser considerados y tratados como información confidencial.

6.2. La red de amplia cobertura geográfica a nivel nacional e internacional debe estar dividida en forma lógica por diferentes segmentos de red, cada uno

separado con controles de seguridad perimetral y mecanismos de control de acceso.

6.3. Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la universidad, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de ciframiento y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

6.4. Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización.

6.5. Las computadoras de la UNEXPO se conectarán de manera directa con computadores de entidades externas, conexiones seguras, previa autorización del grupo de Soporte y Mantenimiento de la Seguridad y/o la OCTSI.

6.6. Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Universidad e Internet deberá estar cifrada

**Política 7: Seguridad para Usuarios Terceros**

7.1. Los dueños de los Recursos Informáticos que no sean propiedad de la Universidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe definir un documento de acuerdo oficial entre las partes.

7.2. Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de UNEXPO para el funcionamiento de recursos que no sean propios de la universidad y que deban ubicarse en sus instalaciones, los recursos serán administrados por la OCTSI.

7.3. Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función y/o servicios, deben ser aprobados por quien será el Jefe inmediato o coordinador. En todo caso deberán firmar el acuerdo de buen uso de los Recursos Informáticos.

7.4. Si se requiere un equipo con módem, este equipo no podrá en ningún momento estar conectado a la Red al mismo tiempo.

7.5. La conexión entre sistemas internos de la universidad y otros de terceros debe ser aprobada y certificada por OCTSI con el fin de no comprometer la seguridad de la información interna de la entidad.

7.6. Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Universidad.

7.7. Como requisito para interconectar las redes de la universidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por la universidad. La universidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La universidad se reserva el derecho de cancelar y

terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la universidad.

**Política 8: Software Utilizado**

8.1. Todo software que utilice la UNEXPO será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la universidad o reglamentos internos.

8.2. Todo el software de manejo de datos que utilice la UNEXPO dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas del mercado para garantizar la integridad de los datos.

8.3. Debe existir una cultura informática en el interior de la Universidad que garantice el conocimiento por parte de los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes que laboran para la UNEXPO, de las implicaciones que tiene el instalar software ilegal en los computadores de la UNEXPO.

8.4. Existirá un inventario de las licencias de software de la UNEXPO que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

8.5. Deberá existir una reglamentación de uso para los productos de software instalado en demostración en los computadores de la UNEXPO.

**Política 9: Actualización de Hardware**

9.1. Cualquier cambio que se requiera realizar en los equipos de cómputo de la universidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del ORTSI.

9.2. La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal técnico de la ORTSI.

9.3. Los equipos de microcomputadores (PC, servidores, LAN entre otros) no deben moverse o reubicarse sin la aprobación previa de la ORTSI y el jefe o coordinador del área involucrada.

**Política 10: Almacenamiento y Respaldo**

10.1. La información que es soportada por la infraestructura de tecnología informática de la UNEXPO deberá ser almacenada y respaldada de acuerdo con las normas emitidas por la OCTSI de tal forma que se garantice su disponibilidad.

10.2. Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

10.3. La UNEXPO definirá la custodia de los respaldos de la información que se realizará externamente con una compañía especializada en este tema.

10.4. El almacenamiento de la información deberá realizarse interna y/o externamente a la universidad, esto de acuerdo con la importancia de la información para la operación de la UNEXPO.

10.5. El área dueña de la información en conjunto con la ORTSI definirán la estrategia a seguir para el respaldo de la información.

10.6. Los funcionarios públicos son responsables de los respaldos de su información en los microcomputadores, siguiendo las indicaciones técnicas dictadas por la ORTSI. La ORTSI será la autorizada para realizar el seguimiento y control de esta política.

**Política 11: Contingencia**

11.1. La OCTSI debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación entre otro.

**Política 12: Auditoria**

12.1. Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la universidad, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoria.

12.2. Todos los archivos de auditorias deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

12.3. Todos los archivos de auditorias de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

12.4. Todos los archivos de auditorias deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.

12.5 Todos los computadores de la Universidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

**Política 13: Seguridad Física**

13.1. La universidad deberá contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las dependencias que la universidad considere críticas.

13.2. Los visitantes a las oficinas de la universidad deben ser escoltados durante todo el tiempo por un empleado autorizado, asesor o contratista. Esto significa que se requiere de un escolta tan pronto como un visitante entra a un área y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta incluyendo clientes, antiguos empleados, miembros de la familia del trabajador.

13.3. Siempre que un trabajador se de cuenta que un visitante no escoltado se encuentra dentro de áreas restringidas de la universidad, el visitante debe ser inmediatamente cuestionado acerca de su propósito de

encontrarse en área restringida e informar a los responsables de la seguridad del edificio.

13.4. Los centros de cómputo o áreas que la universidad considere criticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

13.5. Toda persona que se encuentre dentro de la universidad deberá portar su carnet de identificación en un lugar visible.

13.4. En los centros de cómputo o áreas que la universidad considere criticas deberán existir elementos de control de incendio, inundación y alarmas.

13.5. Los centros de computo o áreas que la entidad considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas

13.6. La Sala de Cableado y Servidores, deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

13.7. Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la universidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la ORTSI.

13.8. Todos los visitantes deben mostrar identificación con fotografía y firmar antes de obtener el acceso a las áreas restringidas controladas por la entidad.

13.9. Los equipos de microcomputadores (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa de la ORTSI, el departamento de Bienes Nacionales y la oficina o unidad dueño del equipo.

13.10. Los funcionarios públicos se comprometen a NO utilizar a la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de computo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipos que generen caídas de la energía.

13.11. Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no están autorizados para utilizar los recursos informáticos de la entidad.

**Política 14: Escritorios Limpios**

14.1. Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, USB memory key, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

**Política 15: Administración de La Seguridad**

15.1. La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada dos años.

Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

15.2. Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (Rectorado, Vicerrectorado) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al encargado de la Seguridad Informática de la OCTSI.

15.3. Los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes que laboran para la UNEXPO que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los Recursos Computacionales. La implementación debe ser consistente con las prácticas establecidas por la ORTSI.

15.4. La OCTSI, divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a el/la Rector(a) de la UNEXPO, los casos de incumplimiento con copia a las oficinas de Auditoria de la UNEXPO.

# ANEXO I. VERIFICACIÓN DE VULNERABILIDADES

| VULNERABILIDADES FISICAS, ORGANIZACIONALES Y OPERACIONALES VERIFICADAS | | | |
|---|---|---|---|
| **Nro.** | **Nivel** | **Descripción** | **Verificación** |
| **1.1** | | **SEGURIDAD LOGICA** | |
| **1.1.1** | | **Identificación** | |
| 1.1.1.1 | 1 | Datos del perfil de usuarios dados de alta | V |
| 1.1.1.2 | 2 | Gestión de bajas de usuarios | V |
| 1.1.1.3 | 2 | Mantenimiento de cuentas | V |
| 1.1.1.4 | 2 | Manejo de los permisos para los accesos | V |
| 1.1.1.6 | 1 | Identificación única o grupal | V |
| 1.1.1.7 | 1 | Gestión de grupos | V |
| 1.1.1.8 | 2 | Superusuario | V |
| 1.1.1.9 | 1 | Visualización del logeo en pantalla | N |
| **1.1.2** | | **Autenticación** | |
| 1.1.2.1 | 2 | Manejo de los datos de autenticación | V |
| 1.1.2.2 | 1 | Manejo de intentos de logeo | V |
| **1.1.3** | | **Contraseñas** | |
| 1.1.3.1 | 2 | Generación de contraseñas | MV |
| 1.1.3.2 | 1 | Gestión de cambio de contraseñas | MV |
| **1.1.4** | | **Control de acceso lógico** | |
| 1.1.4.1 | 1 | Modelo y aplicación | V |
| 1.1.4.2 | 2 | Criterios de acceso | V |
| 1.1.4.3 | 3 | Mecanismos de control de acceso interno | N |
| 1.1.4.4 | 3 | Control de acceso externo | V |
| **1.2** | | **SEGURIDAD EN LAS COMUNICACIONES** | |
| **1.2.1** | | **Configuración de la red** | |
| 1.2.1.1 | 3 | Comunicaciones vía modem | V |
| 1.2.1.2 | 2 | Recursos compartidos de discos de PC | V |
| 1.2.1.3 | 1 | Estado de puertos de servicios no necesarios | V |
| **1.2.2** | | **Virus y Antivirus** | |
| 1.2.2.1 | 3 | No está habilitado para envío y recepción de mail | V |
| 1.2.2.2 | 2 | Actualizaciones no adecuadamente frecuentes | V |
| 1.2.2.3 | 2 | No es suficiente la frecuencia de escaneado de las unidades de las computadores | V |
| 1.2.2.4 | 1 | No se generan discos de rescate en las PCs bajo Win | V |
| **1.2.3** | | **Documentación, normas** | |
| 1.2.3.1 | 1 | Grado y detalle de la información documentada de la red | MV |
| 1.2.3.2 | 2 | Gestión y procesos de parches | V |

| VULNERABILIDADES FISICAS, ORGANIZACIONALES Y OPERACIONALES VERIFICADAS | | | |
|---|---|---|---|
| **Nro.** | **Nivel** | **Descripción** | **Verificación** |
| 1.2.3.3 | 1 | Documentación de la configuración de las PCs | MV |
| **1.2.4** | | **Ataques a la red** | |
| 1.2.4.1 | 1 | Antecedentes de ataques ocurridos a la red | MV |
| **1.2.5** | | **Firewall** | |
| 1.2.5.1 | 3 | Tipo, configuración y nivel de control de firewall | V |
| 1.2.5.2 | 1 | Pruebas de configuración de firewall | V |
| **1.2.5** | | **Máquinas de Fax** | |
| 1.2.5.1 | 2 | Control de envíos por fax | V |
| 1.2.5.2 | 1 | Distribución de faxes recibidos | V |
| **1.3** | | **SEGURIDAD EN LAS APLICACIONES** | |
| **1.3.1** | | **Sistema Operativo** | |
| 1.3.1.1 | 1 | Requisitos de seguridad considerados al elegir el sistema operativo | V |
| **1.3.2** | | **Control de datos de aplicaciones** | |
| 1.3.2.1 | 1 | Existencia de control de cambios para archivos de sistema o bases de datos | V |
| 1.3.2.2 | 3 | Confidencialidad de datos de laptops y notebooks | N |
| 1.3.2.3 | 2 | Logs de transacciones y sus detalles | V |
| **1.3.3** | | **Control de datos en el desarrollo** | |
| 1.3.3.1 | 1 | Existencia de control de cambios para el desarrollo | N |
| 1.3.3.2 | 1 | Control del contenido de archivos de entrada | V |
| 1.3.3.3 | 2 | Control de validez de datos ingresados manualmente | V |
| 1.3.3.4 | 1 | Control de consistencia de datos de salida | MV |
| **1.3.4** | | **Seguridad de bases de datos** | |
| 1.3.4.1 | 2 | Control de acceso propio de las bases de datos | V |
| 1.3.4.2 | 1 | Control de instancias de uso | V |
| 1.3.4.3 | 1 | Chequeo regulares de seguridad | V |
| 1.3.4.4 | 1 | Marcado o borrado de archivos eliminados | V |
| **1.3.5** | | **Control de aplicaciones** | |
| 1.3.5.1 | 2 | Controles con que se realiza la instalación y actualización de parches | V |
| 1.3.5.2 | 1 | Documentación de la instalación o actualización de software | V |
| 1.3.5.3 | 2 | Control de aplicaciones en máquinas de usuarios | V |
| 1.3.5.4 | 1 | Control de información que bajan los usuarios de la Web | V |
| **1.3.6** | | **Mantenimiento de aplicaciones** | |
| 1.3.6.1 | 1 | Documentación de cambios de emergencia | V |
| 1.3.6.2 | 1 | Control regular de programas y servicios innecesarios | V |

| VULNERABILIDADES FISICAS, ORGANIZACIONALES Y OPERACIONALES VERIFICADAS | | | |
|---|---|---|---|
| **Nro.** | **Nivel** | **Descripción** | **Verificación** |
| 1.3.6.3 | 1 | Gestión de cambios complejos en archivos de configuración | V |
| 1.3.6.4 | 2 | Registro de cambios en las configuraciones | V |
| **1.3.7** | | **Ciclo de vida** | |
| 1.3.7.1 | 1 | Metodología usada para el desarrollo | V |
| 1.3.7.2 | 2 | Manejo del código fuente y documentación con desarrollos por terceros | V |
| 1.3.7.3 | 1 | Uso métricas en el desarrollo | V |
| 1.3.7.4 | 1 | Registros históricos de las modificaciones | V |
| 1.3.7.5 | 2 | Existencia de requisitos de seguridad | V |
| 1.3.7.6 | 1 | Medidas de seguridad durante las implementaciones | V |
| 1.3.7.7 | 1 | Forma y documentación de pruebas | V |
| 1.3.7.8 | 1 | Metodología usada para el mantenimiento | V |
| 1.3.7.9 | 1 | Detalles de la documentación generada en el desarrollo | V |
| **1.4** | | **SEGURIDAD FISICA** | |
| **1.4.1** | | **Control de acceso al centro de cómputos** | |
| 1.4.1.1 | 2 | Restricción de acceso a personas ajenas al área | V |
| 1.4.1.2 | 1 | Control personal de limpieza en locales con servidores | N |
| **1.4.2** | | **Control de acceso a los equipos de los usuarios** | |
| 1.4.2.1 | 2 | Habilitación del NetBIOS | V |
| 1.4.2.2 | 1 | Habilitación y control de dispositivos externos | V |
| 1.4.2.3 | 3 | Control de virus | MV |
| 1.4.2.4 | 2 | Existencia de grabadoras de CD | V |
| 1.4.2.5 | 1 | Agregado no autorizado de dispositivos externos | V |
| 1.4.2.6 | 2 | Control y revisión de dispositivos instalados en las PCs | V |
| 1.4.2.7 | 1 | Apagado o no de los servidores | MV |
| **1.4.3** | | **Utilidades de soporte** | |
| 1.4.3.1 | 2 | Gestión de fallas dispositivos externos al funcionamiento del equipamiento IT | V |
| **1.4.4** | | **Estructura del edificio** | |
| 1.4.4.1 | 1 | Tipo, condiciones e instalación del cableado de red | V |
| 1.4.4.2 | 1 | Falta de información de otras instalaciones que corran en paralelo | V |
| 1.4.4.3 | 1 | Actividades que pueden afectar las operaciones | V |
| 1.4.4.4 | 1 | Actividades externas que pueden afectar las operaciones | V |
| 1.4.4.5 | 2 | Protecciones antirrayos | V |

| VULNERABILIDADES FISICAS, ORGANIZACIONALES Y OPERACIONALES VERIFICADAS | | | |
|---|---|---|---|
| **Nro.** | **Nivel** | **Descripción** | **Verificación** |
| **1.4.5** | | **Clasificación de datos y hardware** | |
| 1.4.5.1 | 1 | Forma de rotular computadoras y periféricos | V |
| 1.4.5.2 | 1 | Inventario de recursos de hardware y software | V |
| **1.4.6** | | **Backup** | |
| 1.4.6.1 | 2 | Frecuencia de backups | V |
| 1.4.6.2 | 2 | Datos que se backapean | V |
| 1.4.6.3 | 2 | Tipos de backup que se realizan | V |
| 1.4.6.4 | 2 | Medios de almacenamiento de backups | V |
| 1.4.6.5 | 1 | Rotación de medios | V |
| 1.4.6.6 | 1 | Herramientas de backup | V |
| 1.4.6.7 | 2 | Responsables del backup | V |
| 1.4.6.8 | 1 | Procedimientos de backup | V |
| 1.4.6.9 | 2 | Pruebas periódicas de recuperación | V |
| 1.4.6.10 | 2 | Lugar de almacenamiento y controles de acceso | V |
| 1.4.6.11 | 1 | Rotulación y documentación de backups | V |
| **1.5** | | **ADMINISTRACION DEL CENTRO DE COMPUTOS** | |
| **1.5.1** | | **Contramedidas** | |
| 1.5.1.1 | 1 | Tipo y regularidad de chequeos | MV |
| 1.5.1.2 | 2 | Planificación y documentación de actividades del área | MV |
| 1.5.1.3 | 1 | Documentación detallada del equipamiento | MV |
| 1.5.1.4 | 2 | Documentación y manuales de procedimientos y seguridad | MV |
| **1.5.2** | | **Responsabilidad del equipo de seguridad** | |
| 1.5.2.1 | 3 | Administración de emergencias | MV |
| **1.6** | | **REGISTROS Y AUDITORIAS** | |
| **1.6.1** | | **Auditorias generales** | |
| 1.6.1.1 | 2 | Realización y objetos auditados | V |
| 1.6.1.2 | 1 | Monitoreo y herramientas | V |
| 1.6.1.3 | 2 | Gestión de logs | V |
| 1.6.1.4 | 1 | Utilidad auditoría para rastreo de acciones | V |
| 1.6.1.5 | 1 | Históricos generados | V |
| **1.6.2** | | **Logs** | |
| 1.6.2.1 | 3 | Control de acceso | V |
| 1.6.2.2 | 2 | Identificación y almacenamiento | V |
| 1.6.2.3 | 2 | Información contenida en los logs | V |
| 1.6.2.4 | 1 | Análisis que se realiza | V |

| VULNERABILIDADES FISICAS, ORGANIZACIONALES Y OPERACIONALES VERIFICADAS | | | |
|---|---|---|---|
| **Nro.** | **Nivel** | **Descripción** | **Verificación** |
| **1.6.3** | | **Auditoría de servidores** | |
| 1.6.3.1 | 1 | Trabajos de mayor uso CPU y memoria | V |
| 1.6.3.2 | 1 | Datos de mayor tráfico, CPU y memoria | V |
| 1.6.3.3 | 1 | Aplicaciones de mayor tráfico, CPU y memoria | V |
| **1.6.4** | | **Auditoría de control de acceso** | |
| 1.6.4.1 | 2 | Existencia de logs | V |
| 1.6.4.2 | 2 | Almacenamiento y acceso | V |
| 1.6.4.3 | 1 | Duración y tratamiento posterior al vencimiento | V |
| 1.6.4.4 | 2 | Contenido de los logs | V |
| **1.6.5** | | **Auditoría de redes** | |
| 1.6.5.1 | 1 | Monitoreo de red | V |
| 1.6.5.2 | 1 | Periodicidad de chequeos | V |
| 1.6.5.3 | 1 | Datos revisados y estadísticas | V |
| **1.7** | | **PLAN DE CONTINGENCIAS** | |
| **1.7.1** | | **Plan de contingencias** | |
| 1.7.1.1 | 2 | Existencia, justificaciones | MV |
| 1.7.1.2 | 1 | Alcance del plan | MV |
| 1.7.1.3 | 2 | Responsabilidades y entrenamiento | MV |
| 1.7.1.4 | 2 | Documentación | MV |
| **1.7.2** | | **Plan de recuperación de desastres** | |
| 1.7.2.1 | 3 | Responsabilidades | V |
| 1.7.2.2 | 2 | Identificación de funciones críticas | V |
| 1.7.2.3 | 2 | Grupo y responsable | V |
| 1.7.2.4 | 2 | Inventario de equipamiento | V |
| **1.7.3** | | **Administradores de aplicaciones y sistemas** | |
| 1.7.3.1 | 1 | Personal de desarrollo | V |
| 1.7.3.2 | 2 | Técnicos | V |
| 1.7.3.3 | 2 | Administradores de Redes | MV |
| **1.7.4** | | **Gerencia en seguridad** | |
| 1.7.4.1 | 3 | Visón y compromiso general y medio en la seguridad | V |
| 1.7.4.2 | 3 | Reglas de seguridad | MV |
| 1.7.4.3 | 1 | Personal en general - procedimientos | V |
| 1.7.4.4 | 2 | Personal de desarrollo - procedimientos | V |
| 1.7.4.5 | 3 | Técnicos - procedimientos | V |
| 1.7.4.6 | 3 | Administradores de redes - procedimientos | MV |

| RESUMEN VERIFICACIÓN VULNERABILIDADES | |
|---|---|
| Total de vulnerabilidades potenciales | 109 |
| Vulnerabilidades no presente | 5 |
| Vulnerabilidades de nivel 1 | 55 |
| Vulnerabilidades de nivel 2 | 42 |
| Vulnerabilidades de nivel 3 | 7 |
| Nivel Relativo de Vulnerabilidad Total | 160 |

| VULNERABILIDADES VERIFICADAS LINUX | | | |
|---|---|---|---|
| **N°** | **Nivel** | **Vulnerabilidades** | **S1** |
| **2.1** | | **SERVICIOS ACTIVOS INNECESARIOS** | |
| 2.1.1 | 2 | Hay habilitados servicios innecesarios | V |
| **2.2** | | **Bind/DNS** | |
| 2.2.1 | 2 | Instalación/ISC, versión y parches | V |
| 2.2.2 | 2 | Actualización dinámica del DNS | V |
| 2.2.3 | 2 | Demonio named habilitado en servidores no DNS | V |
| **2.3** | | **RPC** | |
| 2.3.1 | 3 | RPC Habilitado | V |
| 2.3.3 | 2 | Servicios RPC que se pueden explotar | V |
| **2.4** | | **SNMP** | |
| 2.4.1 | 2 | Versión y puertos habilitados | V |
| 2.4.2 | 3 | Nombres comunidad por default | V |
| 2.4.3 | 2 | Chequeo registros MIB | V |
| **2.5** | | **Shell seguro** | |
| 2.5.1 | 1 | Instalación y versión | V |
| **2.6** | | **Servicios NIS/NFS** | |
| 2.6 .1 | 3 | Versión NIS | V |
| 2.6 .2 | 3 | Ubicación password del root con NIS | V |
| 2.6 .3 | 2 | Versión NFS | V |
| 2.6 .4 | 3 | Configuración archivo export y montaje de sistema de archivos NFS | V |
| **2.7** | | **Open SSL** | |
| 2.7.1 | 1 | Versión | V |
| **2.8** | | **FTP** | |
| 2.8.1 | 3 | Habilitación y funcionalidad anónima | V |
| 2.8.2 | 3 | Sin uso de password en el modo de subida | V |
| 2.8.3 | 3 | No hay restricciones y mecanismos para direcciones IP o dominios | V |
| 2.8.4 | 3 | No se usan restricciones propias del servidor ftp | N |
| 2.8.5 | 3 | Especificación de las cuentas administrativas en archivo ftpusers | V |
| 2.8.6 | 3 | No hay diferenciación archivos contraseñas con los del OS | V |
| 2.8.7 | 2 | Permisos y propietarios del raíz y subdirectorios etc y bin del ftp anónimo | N |
| 2.8.8 | 2 | Permisos y propietarios de archivos de subdirectorios etc y bin | V |
| 2.8.9 | 2 | Permisos y propietarios directorio home ~ftp/ | V |
| 2.8.10 | 3 | Existencia de archivos .rhosts y .forward | V |
| 2.8.11 | 3 | Restricciones de escritura para everyone en directorios ftp y sus archivos | V |
| **2.9** | | **Otras de contraseñas** | |
| 2.9.1 | 2 | Hay cuentas extras con UID 0, o sin contraseñas en el archivo passwd | V |
| 2.9.2 | 3 | tftp habilitado | V |
| 2.9.3 | 3 | tftp necesario pero sin precauciones de acceso restringido | V |
| 2.9.4 | 2 | No se usa un programa para mejorar la elección de contraseñas | V |

| VULNERABILIDADES VERIFICADAS LINUX | | | |
|---|---|---|---|
| **N°** | **Nivel** | **Vulnerabilidades** | **S1** |
| **2.10** | | **Otros Servicios de red** | |
| 2.10.1 | 2 | Permisos y propietarios no adecuados en archivos de servicios de red | V |
| 2.10.2 | 2 | Cron acepta usuarios ordinarios | V |
| 2.10.3 | 3 | Se puede registrar como root en la consola en forma remota | V |
| 2.10.4 | 3 | Terminales no adecuados en el archivo de terminal seguro | V |
| **2.11** | | **Seguridad sistema de archivos** | |
| 2.11.1 | 2 | Archivos .exrc no justificados | V |
| 2.11.2 | 2 | Archivos .forward en directorios home de usuarios | V |
| 2.11.3 | 2 | Umask inadecuado de algunos programas | V |
| 2.11.4 | 2 | Restricciones de acceso no adecuadas en algunos archivos bajo /etc | V |
| 2.11.5 | 3 | Escritura indebida de los archivos log | V |
| 2.11.6 | 2 | Características extendidas (inmutabilidad y sólo anexado) no habilitadas | V |
| 2.11.7 | 2 | Inadecuados permisos, propiedad y grupo de /vmunix | V |
| 2.11.8 | 3 | Archivos que no debieran ser propiedad sino de root, y si /tmp no tiene el sticky-bit | V |
| 2.11.9 | 3 | Archivos o directorios no esperados que son escribibles por cualquiera | V |
| 2.11.10 | 2 | Archivos que no debieran tener seteados el bit SUID o SGID | V |
| 2.11.11 | 2 | Umask inadecuado de algunos usuarios | V |
| 2.11.12 | 2 | Archivos ordinarios en el directorio /dev | V |
| 2.11.13 | 2 | Archivos especiales fuera de /dev | V |
| 2.11.14 | 2 | Archivos ejecutables y sus directorios ascendentes escribibles por grupos o cualquiera | V |
| 2.11.15 | 2 | Archivos sin propietarios | V |
| **2.12** | | **Monitoreo del sistema** | |
| 2.12.1 | 3 | No se han definido los archivos log adecuados para seguridad | V |
| 2.12.2 | 2 | No se usan las extensiones de seguridad de Linux para los archivos log | V |
| 2.12.3 | 3 | Ausencia de registro de las actividades de los administradores | N |
| 2.12.4 | 2 | Falta de control de las modificaciones de archivos de sistema | N |
| **2.13** | | **Servicios de archivos** | |
| 2.13.1 | 2 | Inadecuados permisos y propiedad del archivo /etc/export | V |
| **2.14** | | **Linux** | |
| 2.14.1 | 3 | Parches y actualizaciones | V |

| **Resumen Verificación Vulnerabilidades** | |
|---|---|
| **Servidores** | **S1** |
| **Total vulnerabilidades potenciales** | 55 |
| **Vulnerabilidades no presentes** | 4 |
| **Vulnerabilidades de Nivel 1** | 2 |
| **Vulnerabilidades de Nivel 2** | 28 |
| **Vulnerabilidades de Nivel 3** | 21 |
| **Nivel Relativo de Vulnerabilidad Total** | 65 |
| **Servidores más vulnerables** | |
| **Servidores más vulnerables en el Nivel 3** | |

| VULNERABILIDADES VERIFICADS PLATAFORMAS WINDOWS 2003 SERVER | | | | | | |
|---|---|---|---|---|---|---|
| **N°** | **Nivel** | **Vulnerabilidades** | **S1** | **S2** | **S3** | **S4** |
| **3.1** | | **IIS** | | | | |
| 3.1.1 | 3 | Versión y parches del IIS | V | N | N | V |
| 3.1.2 | 2 | Versiones 4 y 5 del IIS; ACL y directorios | V | N | N | V |
| 3.1.3 | 2 | Habilitación del log del IIS | V | N | N | V |
| 3.1.4 | 3 | WebDav ntdll.dll en IIS 5.0 | V | N | N | V |
| 3.1.5 | 2 | Aplicaciones de muestra en directorios iissamples, iishelp y msadc | V | N | N | V |
| **3.2** | | **SQL Server** | | | | |
| 3.2.1 | 3 | Versión y parches del SQL Server | V | V | V | V |
| 3.2.2 | 2 | Log autenticación servidor SQL | V | V | V | V |
| 3.2.3 | 2 | Cuenta SA, contraseña | V | V | V | V |
| **3.3** | | **Autenticación** | | | | |
| 3.3.1 | 3 | Autenticación, algoritmo usado | V | V | V | V |
| 3.3.2 | 3 | Archivo hashes LM, habilitación autenticación a través de la red | V | V | V | V |
| **3.4** | | **Internet Explorer** | | | | |
| 3.4.1 | 3 | Versión y parches del Internet Explorer | V | V | N | N |
| 3.4.2 | 2 | Nivel seguridad del IE | V | V | N | N |
| **3.5** | | **RAS** | | | | |
| 3.5.1 | 3 | Uso SMB, conectividad NetBios | V | V | V | V |
| 3.5.2 | 2 | Sesión nula, registro anónimo | V | V | V | V |
| 3.5.3 | 3 | Acceso remoto al registry | V | V | V | V |
| 3.5.4 | 3 | rpc y parches | V | V | V | V |
| **3.6** | | **MDAC/RDS** | | | | |
| 3.6.1 | 3 | Versión y parches del MDAC | V | N | V | V |
| 3.6.2 | 2 | Archivo msadcs.dll con NT 4.0 e IIS 3.0 o 4.0 | V | N | V | N |
| 3.6.3 | 1 | Versión y SP del Jet Engine | V | N | V | N |
| **3.7** | | **Windows Scripting Host** | | | | |
| 3.7.1 | 3 | Habilitación del Windows Scripting Host | V | N | N | N |
| 3.7.2 | 1 | Forma de ejecución de scripts | V | N | N | V |
| **3.8** | | **Outlook Express** | | | | |
| 3.8.1 | 2 | Ventana de vista previa del Outlook/Outlook Express | V | V | V | V |
| 3.8.2 | 1 | Restricción zona de seguridad del Outlook Express | V | N | N | V |
| **3.9** | | **Compartición P2P** | | | | |
| 3.9.1. | 3 | Puertos de aplicaciones P2P | V | V | V | N |
| 3.9.2 | 2 | Existencia en disco de archivos propios de P2P | V | V | V | N |
| **3.10** | | **SNMP** | | | | |
| 3.10.1 | 2 | Versión y puertos habilitados del SNMP | V | V | V | V |
| 3.10.2 | 3 | Nombres comunidad por default del SNMP | V | N | V | N |
| 3.10.3 | 2 | Chequeo registros MIB del SNMP | V | V | V | N |
| **3.11** | | **Acceso remoto al registry** | | | | |
| 3.11.1 | 3 | Registros bajo SecurePipeServers | V | N | N | V |

| VULNERABILIDADES VERIFICADS PLATAFORMAS WINDOWS 2003 SERVER | | | | | | |
|---|---|---|---|---|---|---|
| **N°** | **Nivel** | **Vulnerabilidades** | **S1** | **S2** | **S3** | **S4** |
| **3.12** | | **Otros seteados del registry** | | | | |
| 3.12.1 | 3 | Registro Winlogon | V | V | N | N |
| 3.12.2 | 2 | Registro LanMan Print Services, para no poder agregar drivers impresión | V | V | V | V |
| 3.12.3 | 2 | Registro Subsystems, OS/2 y Posix | V | V | V | V |
| 3.12.4 | 2 | Registro bajo EventLog, para que no se vean los logs de aplicaciones y sistema | V | V | V | V |
| 3.12.5 | 2 | Registro Session Manager, atributos recursos compartidos, borrado archivo páginas | V | V | V | V |
| **3.14** | | **Otras cuestiones de contraseñas** | | | | |
| 3.14.1 | 2 | Uso del passfilt.dll | V | V | V | N |
| 3.14.2 | 1 | Uso del syskey.exe | V | V | V | N |
| **3.15** | | **Sistema de archivos** | | | | |
| 3.15.1 | 3 | Se usa FAT | V | V | V | V |
| 3.15.2 | 2 | Grupos Everyone (Todos) y/o Usuarios controlados | V | V | V | V |
| **3.16** | | **Logs de auditoria** | | | | |
| 3.16.1 | 2 | Logs en Event Viewer | V | V | V | V |
| 3.16.2 | 1 | Nombres existentes en registro HKLM\System\CurentControlSer\\Control\Lsa | V | V | V | V |
| **3.17** | | **Utilitarios de cuidado** | | | | |
| 3.17.1 | 2 | Existencia y/o restricciones de acceso de archivos ejecutables de cuidado | V | V | V | N |
| 3.17.2 | 1 | Ubicación de los archivos ejecutables de cuidado | V | V | V | V |
| 3.17.3 | 2 | Existencia del programa rollback.exe | V | N | V | V |
| **3.18** | | **Subsistemas de cuidado** | | | | |
| 3.18.1 | 2 | Existencia de c:\winnt\system32\os2 y subdirectorios | V | V | V | V |
| 3.18.2 | 2 | Archivos del os2 y posix en c:\winnt\system32 | V | V | V | V |
| 3.18.3 | 1 | Registros os2 subsystem for nt | V | V | V | V |

| **Resumen Verificación Vulnerabilidades** | | | | |
|---|---|---|---|---|
| **Servidores** | **S1** | **S2** | **S3** | **S4** |
| **Total vulnerabilidades potenciales** | 43 | 43 | 43 | 43 |
| **Vulnerabilidades no presentes** | 0 | 14 | 12 | 13 |
| **Vulnerabilidades de Nivel 1** | 6 | 3 | 4 | 4 |
| **Vulnerabilidades de Nivel 2** | 21 | 16 | 17 | 15 |
| **Vulnerabilidades de Nivel 3** | 16 | 10 | 10 | 11 |
| **Nivel Relativo de Vulnerabilidad Total** | 96 | 65 | 68 | 67 |
| **Servidores más vulnerables** | *** | | | |
| **Servidores más vulnerables en el Nivel 3** | *** | | | |

## ANEXO J. PROCEDIMIENTOS CORRESPONDIENTES A LOS CONTROLES 6.3.1, A.9.2.3, A.9.3.1 Y A.9.5.4

### SISTEMA DE ADMINISTRACIÓN DE CONTRASEÑAS
### Procedimiento correspondiente al control 9.5.4

### 1. Objetivo

Este procedimiento responde a la implementación de las Normas de Aplicación de Uso aceptable, contraseñas y contraseñas de Bases de Datos.

El objetivo de este procedimiento es impedir el acceso no autorizado al computador. Para ello los mecanismos de seguridad del nivel operativo deben utilizarse para restringir el acceso a los recursos del computador. Para el caso se trata que el sistema de administración de contraseñas, asegure un nivel adecuado de calidad, conforme lo estipulado por el control 9.3.1 d), o, si los riesgos de la universidad lo justifican, usar un sistema de control de acceso más elaborado como el de desafío y respuesta.

### 2. Alcance

Este procedimiento se aplica al sistema de administración de contraseñas que maneja los accesos a los recursos informáticos en la Universidad Nacional Experimental Politécnica “Antonio José de Sucre”, Vicerrectorado de Puerto Ordaz.

Su uso está previsto por parte de todos los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO.

Para ejecutar este procedimiento se requiere como prerrequisito el conocimiento y aplicación de las normas mencionadas.

### 3. Definición del Proceso

### 3.1 Introducción

Este procedimiento establece las principales características que debe reunir un sistema de administración de contraseñas.

### 3.2 Descripción

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una funcionalidad eficaz e interactiva que garantice contraseñas de calidad (ver control 9.3.1 como guía acerca del uso de contraseñas).

En la mayoría de los casos son los usuarios mismos lo que eligen y mantienen sus propias contraseñas, aunque con algunas aplicaciones podría

darse que la asignación sea hecha por un empleado de la empresa que pudiera tener autoridad para ello.

Para trabajar con un buen sistema de administración de contraseñas se recomienda establecer las condiciones que siguen:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades. Justificar plenamente los posibles casos en que un grupo use una contraseña común.

b) Cuando corresponda, permitir que los usuarios elijan y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar errores de ingreso.

c) Imponer una elección de contraseñas de calidad según lo señalado en el punto 3.2 a) del control 9.3.1.

d) Cuando los usuarios mantengan sus propias contraseñas, imponer cambios en las mismas según lo señalado en el punto 3.2 e) del control 9.3.1.

e) Cuando la elección de una contraseña dependa del usuario y se requiera la intervención del administrador de seguridad (por ejemplo por ser una nueva cuenta, o pérdida de la contraseña anterior), asignarle una contraseña temporaria del tipo OTP, es decir, una contraseña de única vez, para obligarlo de esta manera a que la cambie en su primer registro o log-on (ver control 9.2.3)

f) Mantener un registro de las contraseñas previas del usuario, por ejemplo de los 12 meses anteriores, y evitar la reutilización de las mismas.

g) No mostrar las contraseñas en pantalla cuando se les tipea.

h) Almacenar en forma separada los archivos de contraseñas y los datos de los sistemas de aplicación.

i) Las contraseñas no deben almacenarse de modo que cualquiera las pueda leer (como el caso de /etc/passwd de Unix/Linux), sino encriptada en un archivo especial (como el archivo de contraseñas shadow de Unix/Linux) que no pueda ser leído por los usuarios.

j) En general, no debe haber ningún usuario sin contraseña, lo cual debe verificarse regularmente en el mismo archivo correspondiente (como el caso de /etc/passwd de Unix/Linux). La misma verificación corresponde hacer con archivos de contraseñas de grupos de usuarios (como el archivo /etc/group de Unix/Linux).

k) Almacenar las contraseñas en forma encriptada, utilizando un algoritmo de encriptado unidireccional. Esto se refiere al uso de un sistema de función hash con producción de un compendio o resumen de la contraseña (ver procedimiento de control 10.3.3, punto 3.2)

l) Cuando se instala un software, modificar las contraseñas predeterminada por el vendedor.

m) Luego de una cantidad de intentos fallados (podrían ser tres) respecto a la contraseñas correcta, bloquear la cuenta de forma tal que su desbloqueo sólo puede ser realizado por el administrador de seguridad.

Para dar cumplimiento a este procedimiento, el administrador de seguridad, los administradores de sistemas y de redes, de la ORTSI prepararán un informe para el área de seguridad con su opinión sobre las características y posibilidades de implementar referidas al sistemas de administración de contraseñas, conforme a los trece incisos de arriba, con arreglos a los estipulado en la norma de aplicación de contraseñas. El informe en cuestión se hará en común con los controles 9.2.3 y 9.3.1, con las debidas aclaraciones de las características ya aplicadas para el momento, las que se recomienden implementar y las razones de las que no se recomienden.

En base al material recibido de los administradores mencionados, se prepara un temario a considerar en el Foro de Gestión. Con las recomendaciones y observaciones que surjan, el área de seguridad irá decidiendo los criterios y las diferentes medidas que se apliquen para actualizar el sistema de administración existente.

Las medidas adoptadas por el área de seguridad serán comunicadas en la forma que corresponda al administrador de seguridad, quién procederá a su implementación informando adecuadamente a los administradores de sistemas y/o redes, si fuere necesario.

Adicionalmente, el área de seguridad revisará las medidas decididas por si alguna pudiere incorporarse directamente a la *Norma de Aplicación de Contraseñas*, en cuyo caso promoverá una nueva versión de la misma. Tanto así sea como que no, el área de seguridad comunicará las medidas adoptadas a todo el personal de la UNEXPO aprovechando las sesiones de concientización a que se refiere el control 9.3.1

## 4 Chequeos del proceso y reporte de cumplimiento

El área de seguridad procurará implementar este procedimiento en el menor tiempo posible. Para ello interactuará con los administradores de sistemas y de redes a través del administrador de seguridad, para obtener la información correspondiente, chequeando semanalmente los avances en tal sentido.

El administrador de seguridad informará regularmente al área de seguridad de las tareas realizadas con respecto a este procedimiento.

Regularmente el área de seguridad realizará chequeos para monitorear el estado de implementación de las medidas de control, especialmente una vez definidos y en vigor los criterios que establezca. En caso de verificar

diferencias con respecto a lo establecido, además de promover su regularización informará a la ORTSI.

Regularmente el área de seguridad realizará chequeos para monitorear el cumplimiento de las medidas adoptadas. En caso de verificar diferencias con respecto a lo establecido, además de promover su regularización informará ORTSI o a la Coordinación de Producción y Operaciones.

## 5 Resolución de Problemas

En caso de presentarse criterios incompatibles entre el personal de los grupos de trabajo Soporte Ambiente Operativo y el grupo de Seguridad y control, éste informará al área de seguridad quien tomará a su cargo las cuestiones que sobrevengan hasta llegar a una solución satisfactoria, dejando documentada la información correspondiente a estos trámites.

En caso de cuestiones insalvables entre el grupos de trabajo Soporte Ambiente Operativo y el grupo de Seguridad y control, la situación será resuelta por el Coordinador de Producción y Operaciones, quién deberá dejar adecuadamente documentada la decisión y los motivos correspondientes. Igualmente el área de seguridad informará al Foro Gerencial.

En caso de cuestiones insalvables entre las demás gerencias o áreas de la empresa y el área de seguridad, la situación será elevada a consideración del Foro Gerencial.

## ADMINISTRACIÓN DE CONTRASEÑAS DE USUARIOS
## Procedimiento correspondiente al control 9.2.3

### 1 Objetivo

Este procedimiento responde a la implementación de las Normas de Aplicación de Uso aceptable, contraseñas y contraseñas de Bases de Datos.

El objetivo de este procedimiento es impedir el acceso no autorizado en los sistemas de información. Para el caso se busca controlar la forma general de uso de contraseñas de validación por parte de los usuarios.

### 2. Alcance

Este procedimiento se aplica a la asignación de contraseñas a los diferentes usuarios de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Vicerrectorado de Puerto Ordaz.

Su uso está previsto por parte de todos los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO.

Para ejecutar este procedimiento se requiere como prerrequisito el conocimiento y aplicación de las normas mencionadas.

### 3. Definición del Proceso

### 3.1 Introducción

Este procedimiento establece las condiciones básicas que se recomiendan para controlar la asignación de contraseñas.

### 3.2 Descripción

Las contraseñas constituyen un medio común de validación de la identidad de un usuario para acceder a un sistema o servicio de información. es necesario controlar la asignación de contraseñas a través de un proceso de administración formal, que se recomienda incluya lo siguiente:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo (esto podría incluirse en los términos y condiciones de empleo, ver control 6.1.4).

b) En los casos usuales en que los usuarios manejan sus propias contraseñas, asegurarse que se vean forzados a cambiar inmediatamente la contraseña provisoria segura que se les provee inicialmente. Por otra parte, las contraseñas provisorias que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse luego de una identificación positiva del usuario.

c) Requerir que las contraseñas provisorias otorgadas a los usuarios lo sean de manera segura. Para el caso hay que evitar la participación de terceros o el

uso de mensajes de correo electrónico sin protección (texto en claro). Además, requerir de los usuarios el recibo de la recepción de la contraseña.

Adicionalmente, las contraseñas nunca deben almacenarse en sistemas informáticos sin protección (ver punto 3.2i del control 9.5.4). En los casos que resulte pertinente, se puede considerar el uso de otras tecnologías de mayor fortaleza para la identificación y autenticación de usuarios, como la biométrica (por ejemplo por verificación de huellas dactilares o verificación de firma) o el uso de chip cards (como tarjeta token o token USB).

Para dar cumplimiento a este procedimiento, el administrador de seguridad, los administradores de sistemas y de redes, prepararan un informe para el área de seguridad con su opinión sobre las características y posibilidades de implementar referidas a las instrucciones que deben seguir los usuarios para la asignación de sus respectivas contraseñas, conforme los dos párrafos anteriores, con arreglo a lo estipulado en la Norma de Aplicación de Contraseñas. El informe en cuestión se hará en común con los correspondientes a los controles 9.3.1 y 9.5.4, con las debidas aclaraciones de las características ya aplicadas para el momento, las que se recomienden implementar, y las razones de las que no se recomienden.

En base al material recibido de los administradores mencionados, el área de seguridad presentará un temario a considerar en el Foro de Gestión. Con las recomendaciones y observaciones que surjan, y su propio criterio, el área de seguridad irá decidiendo los criterios y las diferentes medidas que se apliquen a los usuarios para la asignación de sus respectivas contraseñas.

Las medidas adoptadas por el área de seguridad serán comunicadas en la forma que correspondan al administrador de seguridad, quién procederá a la implementación de lo que pudiere corresponder, informando adecuadamente a los administradores de sistemas y/o redes, si fuera necesario.

Adicionalmente, el área de seguridad comunicará la medida adoptada a todo el personal de la UNEXPO por medio de un instructivo sobre Asignación de Contraseñas preparada al efecto. Con el objeto de simplificar el conocimiento y referencia sobre el uso de contraseñas a todo el personal, el área de seguridad podrá incorporar medidas adoptadas a una nueva versión de la Norma de Aplicación de Contraseñas, dejando sin efecto al instructivo mencionado. Tanto en uno como en el otro caso, corresponderá que el área de seguridad proporciones sesiones de concientización a las diferentes áreas de la UNEXPO.

## 4 Chequeos del proceso y reporte de cumplimiento

El área de seguridad procurará implementar este procedimiento en el menor tiempo posible. Para ello interactuará con los administradores de sistemas y de redes a través del administrador de seguridad, para obtener la información correspondiente, chequeando semanalmente los avances en tal sentido.

El administrador de seguridad informará regularmente al área de seguridad de las tareas realizadas con respecto a este procedimiento.

Regularmente el área de seguridad realizará chequeos para monitorear el estado de implementación de las medidas de control, especialmente una vez definidos y en vigor los criterios que establezca. En caso de verificar diferencias con respecto a lo establecido, además de promover su regularización informará a la ORTSI.

Regularmente el área de seguridad realizará chequeos para monitorear el cumplimiento de las medidas adoptadas. En caso de verificar diferencias con respecto a lo establecido, además de promover su regularización informará ORTSI o a la Coordinación de Producción y Operaciones.

## 5 Resolución de Problemas

En caso de presentarse criterios incompatibles entre el personal de los grupos de trabajo Soporte Ambiente Operativo y el grupo de Seguridad y control, éste informará al área de seguridad quien tomará a su cargo las cuestiones que sobrevengan hasta llegar a una solución satisfactoria, dejando documentada la información correspondiente a estos trámites.

En caso de cuestiones insalvables entre el grupos de trabajo Soporte Ambiente Operativo y el grupo de Seguridad y control, la situación será resuelta por el Coordinador de Producción y Operaciones, quién deberá dejar adecuadamente documentada la decisión y los motivos correspondientes. Igualmente el área de seguridad informará al Foro Gerencial.

En caso de cuestiones insalvables entre las demás gerencias o áreas de la empresa y el área de seguridad, la situación será elevada a consideración del Foro Gerencial.

## USO DE CONTRASEÑAS
## Procedimiento correspondiente al control 9.3.1

### 1. Objetivo

Este procedimiento responde a la implementación de las Normas de Aplicación de Uso aceptable, contraseñas y contraseñas de Bases de Datos.

El objetivo de este procedimiento es impedir el acceso de usuarios no autorizado. Para ello se debe concienciar a los usuarios acerca de su responsabilidad en el mantenimiento de controles de acceso efectivos, en este caso los relacionados con el uso de contraseñas.

### 2. Alcance

Este procedimiento se aplica al uso de contraseñas por parte de todo el personal de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Vicerrectorado de Puerto Ordaz.

Su uso está previsto por parte de todos los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO.

Para ejecutar este procedimiento se requiere como prerrequisito el conocimiento y aplicación de las normas mencionadas.

### 3. Definición del Proceso

### 3.1 Introducción

Este procedimiento establece las diferentes características que caracterizan las buenas prácticas en el uso de contraseñas.

### 3.2 Descripción

Las contraseñas constituyen un medio común de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. por la importancia y trascendencia de estas características, es necesario que los usuarios adopten buenas prácticas de seguridad en la elección y uso de dichas contraseñas.

Se recomienda que se notifiquen a los usuarios la necesidad de respetar las siguientes instrucciones:

a) Mantener contraseñas en secreto.

b) Evitar el tener las contraseñas escritas en papel u otro medio, a menos que tal medio pueda guardarse de manera completamente segura, como sería el caso particular para ciertos usuarios en las que las contraseñas se dejan en custodios en un sobre lacrado y guardado con la debida seguridad. Considerar que una contraseña es como una tarjeta de identificación o un cheque al portador.

c) Cambiar las contraseñas siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

d) Elegir contraseñas de calidad, con una longitud mínima de ocho caracteres que:

   1) Sean fácil de recordar

   2) No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, entre otras.

   3) No tengan caracteres idénticos consecutivos o gruidos totalmente numérico o totalmente alfabéticos.

   4) Preferiblemente tengan al menos un carácter que no sea ni letra ni número.

e) Cambiar las contraseñas a intervalos regulares o según el número de acceso (las contraseñas de cuenta con privilegios deben ser modificadas con mayor frecuencia que las contraseñas comunes), y evitar reutilizar o reciclar viejas contraseñas.

f) Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”) en su primer procedimiento de identificación (ver control 9.2.3). esto puede implementarse temporalmente por medio de un instructivo y la concientización correspondiente, hasta que el sistema de administración trabaje con OTP, es decir, contraseñas de única vez, en este caso para el cambio inicial.

g) No incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo aquellas almacenadas en una tecla de función o macro. (teclas programables de función).

h) No compartir las contraseñas individuales de usuario.

i) Para evitar el uso no autorizado de las computadoras portátiles, protegerlas activando la contraseña del buteo del BIOS. Si por algún motivo no se trabaja de esta manera, almacenar en forma encriptada la información sensible. Si tampoco se tampoco se trabaja de esta forma, no almacenar la información sensible en el disco de las portátiles sino en un disquete que pueda guardarse en forma segura en un lugar diferente al de la computadora portátil. Adicionalmente, usar la opción de ahorro de energía activada por medio de una contraseña para interrupciones breves de uso.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere en principio que mantengan contraseñas múltiples, se les puede dar la opción que utilicen una única contraseña de calidad (ver inciso d) siempre y cuando dichos servicios brinden un nivel razonable de protección a las contraseñas almacenadas.

Para dar cumplimiento a este procedimiento, el administrador de seguridad, los administradores de sistemas y de redes, prepararan un informe para el área de seguridad con su opinión sobre las características y posibilidades de implementar referidas al uso de contraseñas por parte de los usuarios, conforme los nueve incisos de arriba, con arreglo a lo estipulado en la Norma de Aplicación de Contraseñas. El informe en cuestión se hará en común con los correspondientes a los controles 9.2.3 y 9.5.4, con las debidas aclaraciones de las características ya aplicadas para el momento, las que se recomienden implementar, y las razones de las que no se recomienden.

En base al material recibido de los administradores mencionados, el área de seguridad presentará un temario a considerar en el Foro de Gestión. Con las recomendaciones y observaciones que surjan, y su propio criterio, el área de seguridad irá decidiendo los criterios y las diferentes medidas que se apliquen al uso de contraseñas por parte de los usuarios.

Las medidas adoptadas por el área de seguridad serán comunicadas en la forma que correspondan al administrador de seguridad, quién procederá a la implementación informando adecuadamente a los administradores de sistemas y/o redes, si fuera necesario.

Adicionalmente, el área de seguridad comunicará la medida adoptada a todo el personal de la UNEXPO por medio de un instructivo sobre *Uso de Contraseñas* preparada al efecto. Con el objeto de simplificar el conocimiento y referencia sobre el uso de contraseñas a todo el personal, el área de seguridad podrá incorporar medidas adoptadas a una nueva versión de la *Norma de Aplicación de Contraseñas*, dejando sin efecto al instructivo mencionado. Tanto en uno como en el otro caso, corresponderá que el área de seguridad proporciones sesiones de concientización a las diferentes áreas de la UNEXPO.

**4. Chequeos del proceso y reporte de cumplimiento**

El área de seguridad procurará implementar este procedimiento en el menor tiempo posible. Para ello interactuará con los administradores de sistemas y de redes a través del administrador de seguridad, para obtener la información correspondiente, chequeando semanalmente los avances en tal sentido.

El administrador de seguridad informará regularmente al área de seguridad de las tareas realizadas con respecto a este procedimiento.

Regularmente el área de seguridad realizará chequeos para monitorear el estado de implementación de las medidas de control, especialmente una vez definidos y en vigor los criterios que establezca. En caso de verificar diferencias con respecto a lo establecido, además de promover su regularización informará a la ORTSI.

Regularmente el área de seguridad realizará chequeos para monitorear el cumplimiento de las medidas adoptadas. En caso de verificar diferencias con

respecto a lo establecido, además de promover su regularización informará ORTSI o a la Coordinación de Producción y Operaciones.

**5. Resolución de Problemas**

En caso de presentarse criterios incompatibles entre el personal de los grupos de trabajo Soporte Ambiente Operativo y el grupo de Seguridad y control, éste informará al área de seguridad quien tomará a su cargo las cuestiones que sobrevengan hasta llegar a una solución satisfactoria, dejando documentada la información correspondiente a estos trámites.

En caso de cuestiones insalvables entre el grupos de trabajo Soporte Ambiente Operativo y el grupo de Seguridad y control, la situación será resuelta por el Coordinador de Producción y Operaciones, quién deberá dejar adecuadamente documentada la decisión y los motivos correspondientes. Igualmente el área de seguridad informará al Foro Gerencial.

En caso de cuestiones insalvables entre las demás gerencias o áreas de la empresa y el área de seguridad, la situación será elevada a consideración del Foro Gerencial.

**REPORTE DE INCIDENTES DE SEGURIDAD**
**Procedimiento correspondiente al control 6.3.1**

## 1. Objetivo

Este procedimiento responde a la implementación de las Normas de Aplicación de Uso aceptable, Sensibilidad de la información, Procesos Antivirus, Contraseñas, Acceso Remoto, Acceso Discado, Comunicaciones Inalámbricas, VPNs, DMZ Internet y Extranet.

El objetivo de este procedimiento es asegurar que todo los funcionarios públicos (Administrativo, Docente y Obrero), contratistas y pasantes de laboran para la UNEXPO estén concientizados de la necesidad que cualquier incidente que pueda estar relacionado con la seguridad sea notificado al personal competente para registrar estos eventos y tomar decisiones al respecto. Y que esta es la forma natural de reducir los posibles daños en los sistemas aprendiendo de los mismos a tomar las medidas pertinentes para evitar o reducir la posibilidad de su repetición.

## 2. Alcance

Este procedimiento se aplica a los incidentes de seguridad que pudiera afectar a los activos operacionales de la Universidad Nacional Experimental Politécnica “Antonio José de Sucre”, Vicerrectorado de Puerto Ordaz.

Su uso está previsto por parte del personal de ORTSI.

Para ejecutar este procedimiento se requiere como prerrequisito el conocimiento y aplicación de las normas mencionadas.

## 3. Definición del Proceso

### 3.1 Introducción

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la Universidad.

Este procedimiento establece las formas de autenticación necesarias para los accesos a través de redes externas...

### 3.2 Descripción

Establecido el hecho que el acceso de usuarios remotos debe estar sujeto a la autenticación, se encuentra que existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros, por ejemplo los métodos basados en el uso de técnicas criptográficas que pueden proveer una autenticación fuerte.

Para el caso es de suma importancia determinar el nivel de protección requerido mediante una evaluación de riesgos. Esto es necesario para la adecuada selección del método.

Dados los niveles de riesgo encontrados, la autenticación de usuarios remotos por medio de nombre y contraseña sólo será permitida como excepción

y sólo por medio de un protocolo de desafío y respuesta como el CHAP, hasta tanto se implemente otro tipo de solución más segura.

La forma de autenticación a usar debe llevarse a cabo utilizando, por ejemplo, una técnica basada en criptografía por medio de tarjetas tokens o tokens USB. Este último sistema se presta también para el uso de firmas digitales (ver control 10.3.3), necesidad que puede surgir en algunos casos.

Otro mecanismo de uso factible es una herramienta como el SSH que además de ofrecer comunicaciones encriptadas también puede trabajar con autenticación de dos claves, similar al usado en firmas digitales.

Incidentalmente se podría utilizar también líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, si es que fuera constante, a fin de constatar el origen de la conexión (ver control 9.4.4).

Los procedimientos y controles de devolución de llamada o dial-back, por ejemplo utilizando módems de dial-back, puede brindar protección contra conexiones no autorizadas y no deseada a las instalaciones de procesamiento de información de la universidad. Este tipo de control autentica la ubicación en un teléfono determinado de un usuario que intenta establecer una conexión con una red de la Unexpo desde locaciones remotas. Debe usárselo complementando la autenticación especifica del usuario, se por medio del método tradicional de nombre y contraseña, o bien por un método del tipo criptográfico.

De una u otra forma hay que tener presente que de aplicarse el control de devolución de llamada, la organización no debe utilizar servicios de red que incluyan desvío de llamadas, os i lo hace, hay que deshabilitar el uso de dichas herramientas para evitar las debilidades asociadas con las mismas. Asimismo, es importante que el proceso de devolución de llamada garantice que se produzca una desconexión real del lado de la Unexpo. Si así no fuera, el usuario remoto podría mantener la línea abierta fingiendo que se ha llevado a cabo la verificación de la devolución de la llamada. Los procedimientos y controles de devolución de llamada deben ser probados exhaustivamente respecto de esta posibilidad.

Para asegurar la consistencia de los datos de autenticación se recomienda usar un servidor de autenticación basado en radius (protocolo abierto) o en Tacacs + (protocolo de cisco).

En los casos en que se vuelva imposible, complicado o difícil que el usuario remoto use un mecanismo de autenticación basado en hardware, se puede usar el protocolo SSL, aunque su uso generalmente está limitado a los servidores Web o de e-mail. La variante TLS como norma abierta del SSL tiene por ventaja principal el hecho de poder controlar la integridad de un mensaje por medio de la función hashing con clave, para lo cual puede generar la clave correspondiente.

Como complemento de este procedimiento, otros dos se refieren a usos específicos de conexiones externas: el 9.8.1 (computación móvil) y el 9.8.2 (Teletrabajo).

**4. Chequeos del proceso y reporte de cumplimiento**

Las diferentes gerencias usuarias informarán al área de seguridad sobre las necesidades de protección de sus respectivas aplicaciones. El área de seguridad pasará la información correspondiente al administrador de seguridad con las recomendaciones básicas a partir de las necesidades de protección.

Cada conexión remota, o grupo de ellas si se diera esta homogeneidad, será analizada por los administradores del área de tecnología dirigidos por el administrador de seguridad. Los resultados podrán ser discutidos en el Foro de Gestión. La adopción final por parte del área de seguridad, implicará que informe al administrador de seguridad de las medidas adoptadas, así como también a la gerencia usuaria correspondiente respecto de la herramienta a implementar y todas las cuestiones posteriores hasta su total funcionamiento.

Mensualmente, en base a los resultados decididos en cada caso, el administrador de seguridad informará regularmente al área de seguridad de las instalaciones implementadas, las aprobadas y las que están en proceso de aprobación, así como de las rechazadas con los principales detalles en cada caso. Para cumplir adecuadamente este punto el administrador de seguridad centralizará la documentación de seguridad referida a este procedimiento.

Regularmente el área de seguridad realizará chequeos para monitorear las conexiones externas. En caso de verificar la existencia no prevista de conexiones así como su funcionamiento fuera de las decisiones tomadas, además de promover la regularización de los casos detectados informará a la ORTSI.

**5. Resolución de Problemas**

En caso de presentarse criterios incompatibles entre el personal de los grupos de trabajo Soporte Ambiente Operativo y el grupo de Seguridad y control, éste informará al área de seguridad quien tomará a su cargo las cuestiones que sobrevengan hasta llegar a una solución satisfactoria, dejando documentada la información correspondiente a estos trámites.

En caso de cuestiones insalvables entre el grupos de trabajo Soporte Ambiente Operativo y el grupo de Seguridad y control, la situación será resuelta por el Coordinador de Producción y Operaciones, quién deberá dejar adecuadamente documentada la decisión y los motivos correspondientes. Esta información será comunicada por el área de seguridad a la gerencia usuaria correspondiente.

## ANEXO K. CRONOGRAMA DE IMPLEMENTACIÓN DEL SGSI

| Fase | Pasos | Actividad | Semanas |
|---|---|---|---|
| Plan | Paso 1 | **Alcance del SGSI** | 1 y 2 |
| | Paso 2 | **Política General de Seguridad** | 2 y 3 |
| | Paso 3 | **Identificación y valuación de riesgos** | |
| | | a) Identificar y verificar activos. Asignación de niveles | 3, 4 y 5 |
| | | b) Identificación amenazas potenciales. Asignación de niveles | 5 y 6 |
| | | c) Identificación y vulnerabilidades organizacionales y operacionales. Entrevistas, cuestionarios, repreguntas | 7, 8, 9 y 10 |
| | | d) Inspección e identificación de vulnerabilidades físicas. Asignación de niveles | 9 y 10 |
| | | e) Identificación y verificación de vulnerabilidades del Sistema IT | 11, 12, 13 y 14 |
| | | f) Determinación de riesgos servidores y componente activos IT | 15 y 16 |
| | | g) Determinación de riesgo resto de los activos | 17 y 18 |
| | | h) Resumen riesgos y cruces Amenazas Vs. Vulnerabilidades de servidores | 19 |
| | | i) Resumen riesgos y cruces. Amenazas Vs. Vulnerabilidades del resto de los activos | 20 |
| | Paso 4 | Normas de aplicación. Redacción, consulta, vigencia provisoria | 21, 22 y 23 |
| | Paso 5 | Selección objetivos de control y controles de seguridad | |
| | | a) Análisis GAP | 23 y 24 |
| | | b) Determinación de la SoA (Declaración de Aplicabilidad) | 25 |
| | Paso 6 | **Directivas administrativas** | 26 y 27 |
| Do | Paso 7 | **Implementación de controles y contramedidas** | 26 al 37 |
| | Paso 8 | **Concientización y capacitación** | 31 al 37 |
| Check | Paso 9 | **Monitoreo y revisión eficiencia** | 35 al 40 |
| Act | Paso 10 | **Mantenimiento y mejoramiento** | 39 al 44 |

## ANEXO L. CURRÍCULUM VITAE DE LA AUTORA

### CURRÍCULO VITAE

Yaneisy Sofía Tersek Rodríguez, Titular de la Cédula de Identidad N°: V- 8.510.895, de nacionalidad: Venezolana, nació en Barquisimeto Estado Lara el 14 de enero de 1969. Curso estudios superiores en la Universidad "Fermín Toro" de Cabudare Estado Lara obteniendo el Título de Ingeniero en Computación el 27/07/1995 y estudios de Postgrado en la misma universidad obteniendo el título de Magíster en Educación Superior, Mención: Docencia Universitaria el 11/09/2003.

### CURSOS DE PERFECCIONAMIENTO PROFESIONAL

- ✓ Seminario Taller Gestión y Auditoria de la Seguridad de Información Normas ISO 17799 (2005) ISO 27001, Taller de implementación basado en una experiencia real (2007)
- ✓ CCNA, módulo I y II (2007)
- ✓ Implantación de un Sistema de Gestión de Seguridad de Información. ISO 27001:2005 (2006)
- ✓ Administración de Linux en Desktop y Servidores (2006)
- ✓ Capacitación Pedagógica en la Educación Superior, (2006)
- ✓ Como Escribir para Publicar, (2005)
- ✓ Jornada de Construcción Curricular del Programa de Formación en Tecnología de Producción Agroalimentaria, (2005)
- ✓ Diseño e Implementación de Protocolos de Comunicación y Aplicaciones Multimedia Orientado a QoS, (2004)
- ✓ Redes de Alta Velocidad, (2004)
- ✓ Fundamentos de las Tecnología de Redes, (2003)
- ✓ Lenguaje de Alto Nivel, (2003)
- ✓ Metodología de la Investigación Proyecto Factible, (2003)
- ✓ Programación de Páginas Web (I Módulo), (2003)
- ✓ Comunicación Efectiva, (2003)
- ✓ Mapas Mentales, (2003)
- ✓ Programador en Visual Basic 6.0 (2003)
- ✓ Redes en Windows NT, (2003)
- ✓ Mantenimiento de Micro (2003)
- ✓ Profesor en Línea, (2002)
- ✓ Visual FOX PRO, (2001)
- ✓ Operador de Windows Plus, (2000)
- ✓ Redes Informáticas, (1999)
- ✓ Mantenimiento de Microcomputador, (1998)
- ✓ Diseño, Desarrollo y Programación de Sistemas en FoxPro para Windows , (1997)
- ✓ Internet, (1997)
- ✓ Introducción a la computación, (1997)
- ✓ I Seminario de Interactividad 96, Multimedia e Internet, (1996)

## EXPERIENCIA LABORAL

Actualmente desempeña los cargos de Docente Ordinario de la cátedra de Computación y Jefe de la Oficina Regional de Tecnología y Servicios de Información, ORTSI, de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" UNEXPO, Vicerrectorado de Puerto Ordaz.

Se desempeñó en los siguientes cargos:

✓ Docente Contratado en las cátedras de: Introducción a la Informática y Análisis de Sistemas Mecanizados, en el Instituto Universitario de Tecnología de Yaracuy (IUTY), San Felipe Estado Yaracuy. Desde 2001 hasta 2005.

✓ Docente Ordinario, categoría Asistente en las cátedras de: Informática Aplicada I y II, Computación I y II, Introducción la Informática, Programación I, Teleprocesos, Estadística II, Electrónica Digital, Análisis Matemático I, Electiva I y II, Electrónica I, Instituto Universitario de Tecnología "Antonio José de Sucre" (IUTAJS Ext. Yaracuy), desde 2000 hasta 2005.

✓ Coordinadora de Soporte Operativo, en COLORIFICIO PORDECAR C.A. Yaritagua Estado Yaracuy en el 2003 Hasta 2005

✓ Jefe de Sistema y Soporte Técnico, en ELECTROPLOM S.R.L., San Felipe Estado Yaracuy, desde 1996 hasta 2001

✓ Docente Contratado en las cátedras de: Introducción a la Informática y Análisis de Sistemas Mecanizados, en la Fundación Pro-Instituto Universitario de Tecnología de Yaracuy (IUTY), San Felipe Estado Yaracuy. Desde 1998 hasta 2000.

✓ Docente contratado en las asignaturas: Programación II, Base de Datos I, Organización y Métodos, Teleprocesos y Teleprocesamiento de Datos en el Colegio Universitario de Administración y Mercadeo (C.U.A.M.), de San Felipe Estado Yaracuy, desde 1996 hasta 1998

✓ Docente contratado en las cátedras de: Electrónica Digital, Análisis Matemático I y II, Investigación de Operaciones y Lógica Matemática en el Instituto Universitario de Tecnología "Antonio José de Sucre" (IUTAJS Ext. Yaracuy), desde 1991 hasta 1994.

### Experiencia como Tutor Académico

Se desempeñó como tutor académico en los siguientes trabajos de investigación:

✓ La Comunicación y su relación con la Motivación de los Trabajadores de la Empresa C.A. Destilería Yaracuy, Abril, 2005.

✓ Citogenética Convencional de Leucemias Agudas y Crónicas diagnosticadas en la Unidad Centroccidental de Hematología, Oncología, Inmunología y Banco de Sangre del Hospital Dr. Pastor Oropeza Riera, Marzo 2001 a Junio 2004, Diciembre, 2004.

✓ Evaluación de las actividades que se desarrollan en el almacén de repuestos de la empresa Multi Fruit C.A., Octubre, 2004.

✓ Lineamientos Estratégicos para la Agilización de las Cobranzas en la Empresa Vitalim. C.A., Octubre, 2004

- ✓ Análisis de la Calidad de Servicio del Sub-Programa Ruta Social Extra Urbana de la Fundación para el Desarrollo Social de Yaracuy (FUNDESOY), Octubre, 2003
- ✓ Crisis Económica y Financiera y sus efectos sobre el Banco Mercantil Sucursal, San Felipe – Yaracuy, Mayo, 2003
- ✓ Propuesta de un Manual de Entrenamiento para el personal de Venta de la empresa Multimercado La Mejor, C.A., San Felipe – Yaracuy, Mayo, 2003
- ✓ Análisis del Sistema de Información Gerencial a Implantar en la Empresa Inversora Comunicacional Sorte C.A., Mayo, 2001