UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO
Maestría en Ciencias de la Computación

DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA "ANTONIO JOSE DE SUCRE" SEDE RECTORAL

BARQUISIMETO, MARZO 2.007

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO
Maestría en Ciencias de la Computación

DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA "ANTONIO JOSE DE SUCRE" SEDE RECTORAL

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

AUTOR:
LCDO. MUJICA R. MANUEL A.

TUTOR:
PROF. POLANCO R. WILLIAM R.

BARQUISIMETO, MARZO 2.007

APROBACION DEL TUTOR

En mi carácter de Tutor del trabajo de grado presentado por el Licenciado **Manuel Antonio Mujica Ruiz**, para optar al Grado de **Magíster Scientiarum en Ciencias de la Computación**, Mención **Redes de Computadoras**, considero que dicho Trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado que se designe.

En la Ciudad de Barquisimeto, a los veintiocho días del mes de febrero del dos mil siete.

PROF. POLANCO WILLIAM
7.501.562

DEDICATORIA

A Dios Todopoderoso, nuestro señor Jesús por iluminarme y brindarme sabiduría a lo largo de la investigación y carrera.

A mi abuela (Q.P.D.), quien me formo en los primeros años de mi vida.

A mi madre, por su motivación y amor para el logro de esta meta.

A mi esposa, por su apoyo incondicional y comprensión.

A Maria, Lorena, Sofia, Genesis y Manuela para que este esfuerzo sirva de ejemplo de superación.

A mis tías quienes siempre me han impulsado al logro de mis metas.

A todas aquellas personas que de una u otra forma brindaron animo y fortaleza para seguir adelante en mi desarrollo profesional y que contribuyeron para culminar con éxito esta investigación.

Gracias a todos y mi especial agradecimiento,

AGRADECIMIENTO

A la Universidad Centroccidental Lisandro Alvarado (UCLA) por permitirme adquirir valiosos conocimientos, que servirán de mucho en el desempeño laboral.

Al Ingeniero William Polanco, por su valiosa orientación y dedicación para desarrollar y llegar a feliz término la investigación.

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

A los profesores Euvis Piña, Glennys Clemant y Arsenio Pérez por brindarme su colaboración y orientación en el desarrollo del trabajo de grado y a lo largo de la carrera.

A todos mis sinceros agradecimientos,

INDICE GENERAL

CAPITULO pp.

LISTA DE CUADROS

LISTA DE GRAFICOS

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO
Maestría en Ciencias de la Computación

DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA "ANTONIO JOSE DE SUCRE" SEDE RECTORAL

AUTOR: LCDO. MANUEL MUJICA
TUTOR: PROF. WILLIAM POLANCO
FECHA: MARZO 2.007

RESUMEN

El presente trabajo de investigación se basó en diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral. Esto motivado a diversos incidentes de seguridad en los servicios de información que ocurrieron tales como: ataques de denegación de servicio (DOS) al servidor DNS (Domain Name System), presencia de correo SPAM (correo electrónico basura) de manera cotidiana, pérdida o eliminación involuntaria de información institucional en las computadoras de usuarios administrativos, computadoras infectadas de virus y troyanos, así como también la falta de un plan de seguridad de la información que lograse minimizar los riesgos ante las amenazas en las redes de computadoras. Todo lo anteriormente explicado soportó la premisa de realizar un Plan de Seguridad Informática con el fin de dar respuesta a una problemática real y plantear una solución basada en estándares de seguridad internacionales. La elaboración del estudio se realizó metodológicamente a través de las cuatro fases fundamentales en la formulación de un proyecto factible como son: Fase I Diagnóstico; Fase II Factibilidad; Fase III Diseño del Plan de Seguridad Informática y Fase IV Evaluación del diseño del Plan de Seguridad Informática. Para todas ellas se utilizaron análisis estadísticos y técnicas de recolección y análisis de la información dando como resultado mejoras consolidadas en los aspectos de seguridad de la información del setenta y uno por ciento (71%) y una posición estipulada promedio como "buena" en comparación cualitativa con respecto a las otras universidades tomadas como referencia.

Descriptores: Plan de Seguridad Informática, Estándares de Seguridad, Redes de computadoras.

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO
Maestría en Ciencias de la Computación

DESIGN OF A PLAN OF COMPUTER SCIENCE SECURITY FOR THE EXPERIMENTAL NATIONAL UNIVERSITY POLYTECHNICAL "ANTONIO JOSE OF SUCRE" HOST RECTORAL

AUTHOR: LCDO. MANUEL MUJICA
TUTOR : PROF. WILLIAM POLANCO
DATES : MARZO 2.007

ABSTRACT

The present work of investigation was based on designing a plan of computer science security for the Experimental National University Polytechnical "Antonio José de Sucre" host Rectoral. This motivated to diverse incidents of security in the information services that happened such as: attacks of refusal on watch (DOS) to servant DNS (Domain Name System), presence of mail Spam (electronic mail sweepings) of daily way, loss or involuntary elimination of institutional information in the computers of administrative users, infected computers of virus and troyanos, as well as the lack of a plan of security of the information that managed to diminish the risks before the threats in the networks of computers. All previously explained it supported the premise to make a plan of computer science security with the purpose of giving problematic answer a real one and raising a solution based on international standards of security. The elaboration of the study was made methodologically through the four fundamental phases in the formulation of a feasible project as they are: Phase I Diagnosis; Phase II Feasibility; Phase III Design of the plan of computer science security and Phase IV Evaluation of design the plan of computer science security. For all of them statistical analyses and of harvesting and analyses of the information were used technical giving like result improvements consolidated in the aspects of security of the information of the seventy and one percent (71%) and one stipulated position average like "good" in qualitative comparison with respect to the other universities taken like reference.

Description: Plan of Computer science Security, Standards of Security, Networks of computers.

INTRODUCCION

El concepto de seguridad en informática es poco conocido e impartido a los futuros profesionales de las áreas tecnológicas en las universidades tradicionales de nuestro país, hecho corroborable en los pensa de estudio; sin embargo, se detecta que esta área es neurálgica una vez que se tiene contacto con las organizaciones en el campo laboral, ya que estas toman muy en serio la confidencialidad, autenticación y disponibilidad de la información motivado a que ello representa elementos de éxito a la organización.

De acuerdo con el informe de PandaLabs (2.006), un estudio realizado por una importante empresa de seguridad informática arrojó que el veintiuno por ciento (21%) del correo electrónico que reciben las empresas es Spam[1] y que el cinco por ciento (5%) del tráfico total de la red está infectado por algún tipo de software malicioso. Los empleados utilizan el acceso a internet con fines personales al menos una hora por día en sus trabajos, lo cual se tradujo en pérdidas por lucro cesante para las empresas de más de trescientos ochenta (380) millones de dolares durante el año 2.005. Además, se descubrió que el sesenta y seis por ciento (66%) de las visitas a páginas con contenidos pornográficos se efectúan durante la jornada laboral, no sólo provocando pérdidas sino consumiendo el ancho de banda.

En este sentido, el constante cambio de condiciones y plataformas para el manejo de información, aunado al auge de nuevas tecnologías en el área de sistemas y redes conllevan a una minuciosa revisión de los sistemas de gerencia de seguridad de la información de las empresas para tener directrices claras sobre el ámbito de seguridad.

El trabajo de investigación se basó en diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica “Antonio José de Sucre” sede Rectoral.

En este sentido, el trabajo de investigación se estructuró en seis (6) capítulos: el Capítulo I, conformado por el Problema, en el cual se desarrolla su planteamiento, objetivos de la investigación, justificación e importancia.

---

[1] SPAM: son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. http://es.wikipedia.org/wiki/Spam

El Capítulo II, denominado Marco Teórico, contentivo de los antecedentes de investigación, bases teóricas, bases legales y sistema de variables.

El Capítulo III, Marco Metodológico, contiene la naturaleza y diseño de la investigación con la descripción de las fases del proyecto factible.

El Capítulo IV, Propuesta del Estudio, presenta la fase I: Diagnóstico, fase II: Factibilidad y la fase III: Diseño del Plan de Seguridad Informática

El Capítulo V, Ejecución y Evaluación de la Propuesta, se efectúa la fase IV.

Por último el Capítulo VI, mostrará las conclusiones y recomendaciones de la investigación.

Las teorías que sustentan la investigación son las de ciencias de la computación en la especialidad de redes de computadores y puntualmente en seguridad de la información, utilizando como modalidad metodológica la de proyecto factible. Con estas teorías se pretende soportar el diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral, tomando como referencia la norma ISO/IEC-27001:2005 y la norma ISO/IEC-17799:2005.

CAPITULO I

EL PROBLEMA

Planteamiento del Problema

> "La mayoría de las personas gastan más tiempo y energías en hablar de los problemas que en afrontarlos."
>
> ***Henry Ford***

En las últimas dos décadas del siglo XX y primera del XXI, se han propiciado cambios en el área tecnológica que han impulsado la automatización de los procesos de las distintas organizaciones, siendo uno de estos cambios el uso masivo de redes de computadoras para la transmisión de voz, vídeo y datos. Las redes de computadoras como lo explica Tanenbaum (2.003), "…es un conjunto de computadoras autómatas interconectadas. Se dice que dos computadoras están interconectadas si pueden intercambiar información…". El crecimiento de las redes de computadoras es acelerado por un elemento tecnológico asociado a los nuevos tiempos como lo es el Internet, entendiéndose como la interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente, es decir, cada ordenador de la red puede conectarse a cualquier otro. También se le conoce como la gran red de redes o la súper autopista de la información.

Para lograr la interconexión de las redes se requirió de un modelo que sirviera de marco de referencia. Este fue propuesto por la ISO[2] (Internacional Standards Organization) en la década de los 70's, dándole el nombre de modelo OSI (Open Systems Interconnection) el cual está basado en siete capas, definiendo para cada una

[2] ISO: *International Organization for Standarization (ISO)*, es una organización internacional no gubernamental, compuesta por representantes de los organismos de normalización (ONs) nacionales, que produce normas internacionales industriales y comerciales. http://www.iso.org/

de ellas servicios, interfaces y protocolos a utilizar. Al respecto Bigelow (2.003) explica "…el modelo OSI describe cómo se desplaza la información de una aplicación en un equipo, a través de la red, a la aplicación de otro equipo… este modelo se considera el principal modelo de arquitectura para comunicaciones y es el marco donde encajan los estándares existentes".

Otra de las instituciones que colabora con el ámbito de normalizaciones y estándares es la Comisión Electrotécnica Internacional (IEC por sus siglas inglesas). Esta es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas. Numerosas normas se desarrollan conjuntamente con la ISO y por ello se da el nombre de normas ISO/IEC.

Como consecuencia de establecer un modelo único de referencia, el modelo OSI, ha permitido que el proceso de comunicarse a través de las redes de computadoras evolucione; sin embargo, éste proceso se ve amenazado constantemente por vulnerabilidades que aparecen reiteradamente en los sistemas de información y también como consecuencia de inadecuadas políticas de seguridad o falta de éstas para el manejo de los servicios de información. El problema de seguridad repercute negativamente en el ámbito financiero e incluso en la imagen organizacional, motivado a que este ocasiona pérdida de reputación y confianza.

La Academia Latinoamericana de Seguridad Informática (2.004) destaca al respecto que "la información es el objeto de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación nos presenta un nuevo escenario. La seguridad de la información es un asunto tan importante, pues afecta directamente a los negocios de una empresa o individuo".

Por lo tanto, la relevancia de tener seguridad de información en las redes de computadoras es evidente. Maiwald (2005) explica que "la seguridad de la información son las medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o denegación del uso de conocimientos, hechos, datos o capacidades".

Existen varias normas internacionales que buscan garantizar la seguridad de la información en las organizaciones. De ellas la que se ha tomado como punto de

referencia ha sido la norma ISO/IEC-27001:2005 titulada "Sistemas de gestión de seguridad de la información – Requerimientos". Este documento está destinado a ser utilizado como punto de partida en las organizaciones que deseen implementar seguridad de la información y cuyo origen esta basado en la norma British Standards Institution BS 7799-2, la cual fue usada hasta mediados del año 2.005 como elemento para certificar a las empresas sobre los estándares de seguridad. Este estándar internacional ha sido preparado con la finalidad de proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI).

Además, la norma ISO/IEC-17799:2005 titulada "Código para la práctica de la gestión de la seguridad de la información", establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información. Esta norma es complemento de la ISO/IEC-27001:2005

En este orden de ideas, las Universidades Venezolanas como organizaciones en las cuales se prestan servicios de información han utilizado como parte de sus herramientas tecnológicas las redes de computadores. Es evidente que estas no escapan de los problemas de seguridad de la información planteados con antelación, tal y como se ha podido corroborar por observación directa del investigador en la Universidad Experimental Politécnica "Antonio José de Sucre", en donde, han ocurrido incidentes de seguridad en los servicios de información tales como: ataques de denegación de servicio al servidor DNS (Domain Name System), presencia de correo SPAM (correo electrónico basura) de manera cotidiana, perdida o eliminación involuntaria de información institucional en los computadores de usuarios administrativos, computadores infectados de virus, troyanos y la no existencia de un plan de seguridad de la información que logre minimizar los riesgos ante las amenazas.

Esta Universidad fue creada el 20 de febrero de 1.979, mediante Decreto Ejecutivo No. 3.087, El área tecnológica es dirigida por la Oficina Central de Tecnología y Servicios de Información (OCTSI), creada el 04 de mayo de 2.005 en su sesión extraordinaria no. 2005-E09-05 de Consejo Universitario de la UNEXPO, en

concordancia con los lineamientos de Tecnología y Servicios de Información, aprobado el 20 de julio del 2.004 según resolución de Consejo Universitario No. 2004-E14-06. A ella pertenece el grupo de Seguridad y Control como se muestra en el gráfico 1 y cuyas funciones son:

1. Aplicar y velar por el cumplimiento de las medidas de seguridad en comunicaciones, servicios de información y plataforma tecnológica.
2. Realizar, mantener y garantizar la integridad de la información manejada, a través de procedimientos de respaldos y de seguridad.
3. Aplicar las medidas de seguridad establecidas para la operación y funcionamiento de los recursos tecnológicos y de información de la Institución.
4. Realizar el monitoreo continuo de la seguridad, en la plataforma tecnológica de la institución.
5. Llevar estadísticas sobre intentos de acceso no autorizados a los servicios de información y la red corporativa de datos de la Institución.
6. Implantar normas y procedimientos para la asignación de prioridades y recursos requeridos para la puesta en producción de planes de seguridad.
7. Garantizar la seguridad en el intercambio de información entre los usuarios y los servicios de información en producción.
8. Realizar las actividades que por su naturaleza corresponden al área de soporte y mantenimiento de la seguridad.

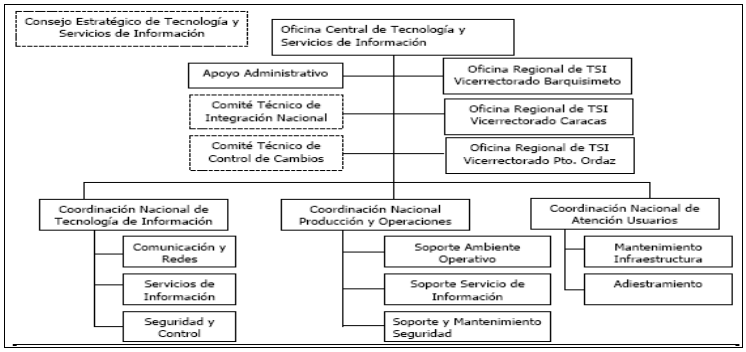


Gráfico 1. Estructura Organizativa Oficina Central de Tecnología y Servicios de Información.
Fuente: Reglamento de Tecnología y Servicios de Información de la UNEXPO (2.005)

Por otra parte, se evidencia un orden jurídico Institucional como son los Lineamientos de Tecnología y Servicios de Información y el Reglamento de Tecnología y Servicios de Información de la UNEXPO, ambos de carácter mandatarios en relación a que deben ser contemplado los aspectos de seguridad de la información dentro de la Universidad.

Con este escenario planteado y de continuar los hechos irregulares presentados dentro de la institución en relación al tratamiento de la información, podrían generarse responsabilidades legales al personal encargado de mantener y administrar la tecnología y servicio de información dentro de la Universidad.

Por lo antes expuesto, se propone diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral y para ello se establece como referencia la norma ISO/IEC-27001:2005 y la norma ISO/IEC-17799:2005. En este punto se hace indispensable analizar minuciosa y detalladamente las respuestas a las siguientes interrogantes:

¿Cómo está actualmente la seguridad informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", en la sede Rectoral?.

¿Cuál es la factibilidad de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral?.

¿Qué características debe tener el diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral?.

¿Cual será el resultado de evaluar el diseño del Plan de Seguridad Informática?.

Las respuestas a estas interrogantes permitirán proponer el diseño del Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral, tomando como referencia la norma ISO/IEC-27001:2005 y la norma ISO/IEC-17799:2005.

Objetivos de la Investigación

Objetivo General

Diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

Objetivos Específicos

- Diagnosticar la situación actual en la que se encuentra la seguridad informática en la Universidad Nacional Experimental Politécnica "Antonio José de Sucre". sede Rectoral.
- Determinar la factibilidad operativa, técnica y económica de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.
- Diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.
- Evaluar el diseño del Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

Justificación e Importancia

El desarrollo de la ciencia de la computación se ha visto afectada favorablemente dado los significativos avances de los últimos treinta (30) años en el ámbito de las telecomunicaciones usando los medios electrónicos informáticos como el Internet y las redes de comunicaciones como forma de masificación de información. Esta masificación ha obligado a los administradores de redes de computadores a incorporarse en la lucha por ofrecer seguridad de la información en los entornos que administran. La información que viaja a través de las redes es susceptible a ser vista,

generada o alterada por terceros. De allí la necesidad de ofrecer seguridad en todos los niveles de información de las organizaciones.

En este sentido, las universidades como organizaciones de servicios deben incorporarse dentro de los estándares que involucren seguridad en la información. Las leyes venezolanas 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.

La Universidad Nacional Experimental Politécnica "Antonio José de Sucre" como universidad pública, se encuentra interesada en brindar seguridad a la información que viaja a través de sus redes de computadores por lo que se ha surgido la necesidad de diseñar un Plan de Seguridad Informática para ella en su sede Rectoral".

Con el diseño propuesto se espera ofrecer una solución efectiva a los problemas de seguridad en la universidad para brindar confiabilidad, confidencialidad y no repudio de la información minimizando los riesgos. También aportar una alternativa para las otras universidades o instituciones con problemática similar. De igual manera, se espera que la investigación sirva como base para futuras investigaciones en el área.

Alcances y Limitaciones

Dentro de los alcances que se tiene es el diseño de Plan de Seguridad Informática tomando como referencia la norma ISO/IEC-27001:2005 e ISO/IEC-17799:2005, se realizará para el caso particular de la red de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" en la sede Rectoral.

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

CAPITULO II

MARCO TEORICO.

Antecedentes de la Investigación

> "Los que se enamoran de la práctica sin la teoría son como los pilotos sin timón ni brújula, que nunca podrán saber a dónde van."
>
> ***Leonardo Da Vinci***

Todo estudio requiere, la revisión de la literatura existente sobre temas relacionados con el trabajo que se elabora, por lo que se hace necesaria la consulta de estudios realizados con el mismo. En el presente capítulo se citan investigaciones que han contribuido a generar antecedentes a la propuesta de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral. Entre los trabajos presentados se destacan los siguientes:

Murillo (2.001) en su trabajo "*Diseño y Aplicación de un Sistema Integral de Seguridad Informática para la Universidad de las Américas (UDLA)"*, tiene como objetivo general de proyecto diseñar y aplicar un esquema integral de seguridad informática basado en un estudio de metodologías de seguridad para satisfacer los requerimientos usuario - infraestructura -administrador de la red de la UDLA. A lo largo de la investigación se presentan los aspectos relevantes de la teoría de seguridad informática aplicada a las necesidades de la red UDLA, conceptos básicos de la seguridad informática, la situación actual de la UDLA. También comprende un análisis del estado del arte en la seguridad informática y los puntos más relevantes sobre la seguridad en el sistema operativo UNIX. Exponen los conceptos más relevantes sobre criptología, firewalls y herramientas existentes describiendo la síntesis de este trabajo: por un lado, el *Hacker´s work bench* como esquema de detección de vulnerabilidades

de la red UDLA y por otro, el *Administrator´s work bench* como esquema de prevención de ataques. Se explican las partes que conforman el esquema de seguridad propuesto, su implantación, sus objetivos, y las necesidades que cubren presentando los resultados obtenidos en el trabajo, el estado actual de los sistemas desarrollados, los beneficios probados en una red local y en la red UDLA. Como conclusión corrobora la necesidad de incluir un área exclusivamente al monitoreo y control de la seguridad informática en cualquier red de cómputo. Por otro lado, las políticas y procedimientos establecidos no son reflejados motivado a su carácter de confidencialidad y por último, se evidencia la existencia de múltiples herramientas gratuitas para implantar seguridad en las redes de computo.

La relación que presenta este trabajo a la propuesta que se está presentando se basa en el diseño y aplicación de un esquema integral de seguridad informática considerando por un lado un estudio de metodologías de seguridad para satisfacer los requerimientos usuario - infraestructura –administrador, y por el otro el uso de los conceptos más relevantes sobre criptología, firewalls y herramientas existentes, así como el *Hacker´s work bench* como esquema de detección de vulnerabilidades de red y el *Administrator´s work bench* como esquema de prevención de ataques.

Cerini y Prá (2.002) desarrollaron una auditoría de seguridad informática y un análisis de riesgos en una empresa de venta de automotores titulado "*Plan de seguridad informática*", con el fin de elevar la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas y el cumplimiento de los reglamentos y normas prescritas. La metodología empleada fue la de investigación de campo dando como resultado las debilidades encontradas y recomendaciones que contribuyen a mejorar su nivel de seguridad. Esto se llevó a cabo como medio para el desarrollo de un plan de seguridad informática, donde se definieron los lineamientos de la planeación, el diseño e implantación de un modelo de seguridad con el objetivo de establecer una cultura de seguridad en la organización.

El propósito de establecer un plan es proteger la información y los activos de la organización, tratando de conseguir confidencialidad, integridad y disponibilidad de los

datos; y las responsabilidades que deben asumir cada uno de los empleados de la organización, hecho relevante para el desarrollo de la presente investigación, ya que aporta una metodología de referencia para realizar un plan de seguridad de información.

Melamed y Ripepi (2.002). desarrollaron un "*diseño e implantación de una arquitectura integrada de protección para la plataforma de correo electrónico en una empresa de telecomunicaciones incluyendo tanto la intranet como extranet"*. El proyecto consistió en diseñar e implantar una arquitectura integrada de protección para el correo electrónico en la Corporación CANTV[3]. Con esta arquitectura se buscó reducir las posibles vulnerabilidades de seguridad. Este trabajo analiza la información manejada en la Corporación con el fin de diseñar políticas y procedimientos de seguridad para los empleados, que permitieron reforzar el esquema de seguridad de la información vía correo electrónico. Como conclusión se logra el diseño e implantación de procedimientos automáticos para la instalación de certificados digitales, y esto permite el intercambio de información segura dentro de la plataforma de correo de la Corporación. Del mismo modo, se automatizó el procedimiento de distribución de las claves públicas y privadas. Con esta actividad se reduce a un 100% la probabilidad de ocurrencia de errores humanos al momento de ejecución de este tipo de actividades y se garantiza el éxito en la implantación de la arquitectura de seguridad para la plataforma de correo en forma uniforme y acorde a los lineamientos establecidos en el trabajo de grado.

El trabajo presentado por Melamed y Ripepi logra establecer conceptos claros y básicos para los aspectos concernientes a la seguridad informática, así como el diseño de políticas y procedimientos de seguridad para los empleados; hecho relevante a la hora de establecer antecedentes de investigación en el área específica.

De Souza (2.002) presentó en la Universidad Federal de Santa Catarina una Tesis titulada "*Gerencia de seguridad de información en sistemas de teletrabajo"*. Como

[3] CANTV: Proveedor de acceso a internet, servicio de acceso vía dial-up y conexiones dedicadas con adsl y frame relay. http://www.cantv.net/

objetivo de la gerencia de seguridad de información, realizó una revisión para verificar como las empresas Brasileras estaban administrando sus programas de teletrabajo con relación a seguridad de información. Como base tomó fundamentos teórico-empíricos y los resultados de investigaciones. La metodología utilizada fue un modelo de seguridad para garantizar la confidencialidad de la información en sistemas de teletrabajo, partiendo de un contexto de acceso remoto o modelo delineado, implementado a partir de la norma ISO/IEC 17799. Los resultados obtenidos, por medio de la aplicación del modelo en una situación real, permitió validar la aplicación de la metodología propuesta como un instrumento efectivo para la gerencia.

La relación de la presente investigación se centra en la utilización de la norma ISO/IEC 17799 para lograr una mejor seguridad de la información en sistemas de teletrabajo. El uso de esta norma es antecedente ineludible de esta investigación.

Hamana (2.003) en su trabajo de grado titulado "*Elementos básicos para modelos de seguridad en organizaciones venezolanas*". Realiza un análisis conceptual sobre seguridad respondiendo las siguientes interrogantes: ¿qué es seguridad?, ¿cuáles son las amenazas y las herramientas con las que se cuenta?. Se enumeran 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 del trabajo, 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. La metodología utilizada fue un estudio del tipo descriptivo no experimental. Dentro de la conclusiones obtenidas se puede considerar que el primer paso a seguir por una empresa para ser segura es identificar los puntos débiles de su red. La realización de tests, estudios detallados de puntos de entrada y análisis de protocolos de aplicaciones pueden formar parte de esta etapa. A partir de los resultados, informe en mano, se procede a evaluar qué áreas requieren mayor trabajo para garantizar que no serán vulneradas por eventuales atacantes.

El modelo de seguridad para la 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.

En definitiva se puede decir, que los trabajos de Murillo, Medina, Melamed y Ripepi exponen un diseño y aplicabilidad de esquemas integrales de seguridad, así como conceptos sólidos y relevantes a la hora de la investigación. Hamana, De Souza, Cerini y Prá contribuyen en lo relacionado a modelos, políticas, lineamientos y normas utilizadas para la implementación de seguridad informática.

En este sentido, es evidente que las investigaciones señaladas guardan una estrecha relación con el objetivo general de este trabajo de grado, tanto en lo relacionado con la seguridad de la información, como en las normativas, políticas y lineamientos necesarios para el resguardo de las mismas.

Bases Teóricas

Entre los enfoques teóricos que sustentan este estudio, se han considerado los supuestos de la Historia, Seguridad, Estándares de Seguridad, Norma ISO/IEC 27001:2005, Norma ISO/IEC 17799:2005, Políticas de Seguridad, Administración del Riesgo, entre otras. En ese sentido, se parte de un enfoque epistemológico sistémico, basado en una teoría que concibe la estructura como una concepción, que según Hurtado (2.000), "es aquella donde la realidad es vista bajo una concepción sistemática, en la cual la integración de elementos cumple funciones y configura estructuras".

Historia

La historia de la seguridad informática se remonta a los tiempos de los primeros documentos escritos. De hecho, la necesidad de información segura tuvo su origen en el año 2.000 antes de Cristo. Como lo explica González (2.003) los egipcios fueron los primeros en utilizar jeroglíficos especiales para codificar la información y, según paso

el tiempo, las civilizaciones de Babilonia, Mesopotámia y Grecia inventaron formas de proteger su información escrita. La codificación de la información, que es el base del cifrado, fue utilizada por Julio Cesar, y durante toda la historia en períodos de guerra, incluyendo las guerras civiles y revolucionarias, y las dos guerras mundiales. Una de las máquinas de codificación mejor conocidas fue la alemana *Enigma*[4], utilizada por los alemanes para crear mensajes codificados en la Segunda Guerra Mundial. Con el tiempo, y gracias a los esfuerzos del proyecto *Ultra* de los Estados Unidos de América, entre otros, la capacidad de descifrar los mensajes generados por los alemanes marcó un éxito importante para los aliados.

En los últimos diez años, la importancia de la seguridad informática se ha puesto de manifiesto por algunas historias. Una de ellas fue la del *gusano de Internet,* en 1.988, que se extendió por decenas de miles de computadores, como resultado de la obra de un *hacker*[5] llamado *Robert Morris.* Había un pirata informático en 1.995 en Alemania que se introdujo en casi 30 sistemas a partir de un objetivo que se había propuesto a sí mismo de casi 500. Más recientemente, en febrero de 1.995, el arresto del pirata informático más buscado, *Kevin Nitnick,* reveló las actividades criminales que incluían el robo de códigos, de información y de otro tipo de datos secretos durante años. Claramente, la amplia utilización de los sistemas informáticos ha puesto en evidencia la importancia de la seguridad informática. El objetivo principal de la seguridad informática es proteger los recursos informáticos del daño, la alteración, el robo y la pérdida. Esto incluye los equipos, los medios de almacenamiento, el software, los listados de impresora y en general, los datos.

---

[4] Enigma: Era una máquina con mecanismo de cifrado rotativo utilizado tanto para cifrado como para descifrado, http://es.wikipedia.org/wiki/Enigma_

[5] Hacker: (del inglés hack, hachar) es el neologismo utilizado para referirse a un experto (véase Gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. http://es.wikipedia.org/wiki/Hacker

Seguridad

Según la Real Academia Española (2.006), lo define "...como estado de seguro; garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo..."

Si se aplica el concepto anterior a seguridad de la información, se debe ampliar el concepto indicando que es una característica de cualquier sistema que indique que este último está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema cien por ciento seguro.

Según Gomez (2.006) para que un sistema se pueda definir como seguro se debe dotar de cuatro características al mismo:

- Integridad: requiere que la información solo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación demensajes trasmitidos.
- Confidencialidad: requiere que la información sea accesible únicamente por las entidades autorizadas.
- Disponibilidad: requiere que los elementos del sistema informático estén disponibles para las entidades autorizadas cuando los necesiten.
- No repudio: ofrece protección a un usuario frente a otro usuario que nieguen posteriormente que se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje.

Por su parte Maiwald (2.005) la define como "Medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso de conocimiento, hechos, datos o capacidades". En definitiva la seguridad de la información es el nombre

dado a los pasos preventivos que se toman para proteger tanto la información como sus capacidades.

Estándares de Seguridad

En lo que respecta a estándares de seguridad, la Universidad Nacional de Colombia y esCERT[6] Universidad Politécnica Catalunya (2.005) exponen que existen varios estándares internacionales relacionados con seguridad informática que se consideran importantes en la actualidad o que deben ser referenciados por su importancia histórica. En este sentido, están clasificados en seis (6) clases de estándares como son: para la administración de seguridad de la información, para evaluación de seguridad en sistemas, para desarrollo de aplicaciones, para servicios financieros, para riesgos y para autenticación.

Para la administración de seguridad de la información:

- La Internet Engineering Task Force (IETF[7]) elaboró el RFC[8] 2196 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. Fue desarrollado por el British Standards Institute.
- La Agencia Federal Para Seguridad de Información en Alemania ha generado el IT Baseline Protection Manual. Este documento presenta un conjunto de

[6] esCERT: Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas. http://escert.upc.es/index.php/web/es/index.html

[7] IETF: **I**nternet **E**ngineering **T**ask **F**orce, en castellano Grupo de Trabajo en Ingeniería de Internet. Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte. http://www.ietf.org/

[8] RFC: Un documento **R**equest **F**or **C**omments (abreviado como **RFC**), que se traduce como "petición de comentarios", es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades. http://www.rfc-editor.org/

métricas de seguridad recomendadas o safeguards, como se denominan en el manual, para sistemas IT típicos.

- La Organización para la cooperación y el desarrollo económicos, en inglés (OECD[9]) creó directrices para la seguridad de sistemas y redes de información. las cuales pueden ser revisadas en Guidelines for the Security of Information Systems.

Estándares para evaluación de seguridad en sistemas:

- La International Organization for Standardization (ISO) ha elaborado el estándar IS 15408. 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.
- La Serie Arco Iris - Rainbow Series- (Orange Book) (EE.UU.) Una importante serie de documentos es la Rainbow Series, que delinea varios estándares de seguridad desarrollados en los Estados Unidos.
- El Reino Unido elaboró el Information Technology Security Evaluation Criteria (ITSEC[10]) a comienzos de los años 90, y es otro estándar históricamente importante. Fue elaborado, en algunos aspectos, basándose en el Orange Book.

Estándares para desarrollo de aplicaciones:

- El Software Engineering Institute lideró el desarrollo del Capability Maturity Model (CMM), que es un método para garantizar madurez en procesos.
- Un derivado del CMM es el System Security Engineering Capability Maturity Model (SSE-CMM). El SSE-CMM describe las características esenciales del proceso de la ingeniería de la seguridad de una organización que deben existir para asegurar la buena ingeniería de la seguridad.

Estándares para servicios financieros:

- ISO 11131:1992 Banking and Related Financial Services; Sign-on Authentication

[9] OECD: Organisation for Economic Co-operation and Development. http://en.wikipedia.org/wiki/OECD

[10] ITSEC: Information Technology Security Evaluation Criteria. http://en.wikipedia.org/wiki/ITSEC

- ISO 13569:1997 Banking and Related Financial Services -- Information Security Guidelines

Estándares para riesgo:

- Acquisition Risk Management (EE.UU.) El Software Engineering Institute tiene algunos documentos sobre Acquisition Risk Management.

Estándares para autenticación:

- ISO 11131:1992 Banking and Related Financial Services; Sign-on Authentication

Debido a la necesidad de establecer seguridad en la información que poseen las organizaciones era preciso la existencia de alguna normativa o estándar que englobase todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudiesen afectarla. Ante esta disyuntiva apareció el BS 7799, o estándar para la gestión de la seguridad de la información, un estándar desarrollado por el British Standard Institute en 1.999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información dentro de la organización. Esta normativa británica generó en la actual ISO/IEC 27001:2005 y la ISO/IEC 17799:2005.

La ISO/IEC 27001:2005 y la ISO/IEC 17799:2005 consideran a la organización como una totalidad y tienen en consideración todos los aspectos que se pueden ver afectados ante los posibles incidentes ha producirse. Estas normas pretenden aportar las bases para tener en consideración todos y cada uno de los aspectos que puede suponer un incidente en las actividades de negocio de la organización.

Esta norma es aplicable a cualquier empresa, sea cual sea el tamaño, la actividad de negocio o el volumen del mismo. Esto es lo que se denomina el principio de proporcionalidad de la norma; es decir, que todos los aspectos que aparecen en la normativa deben ser contemplados y tenidos en cuenta por todas las organizaciones a la hora de proteger sus activos, y la diferencia radicará en que una gran organización tendrá que utilizar más recursos para proteger activos similares a los que puede poseer una pequeña organización. De la misma forma, dos organizaciones que tengan

actividades de negocio muy diferentes, no dedicarán los mismos esfuerzos a proteger los mismos activos de información.

En pocas palabras, esta norma debe tenerse como guía de los aspectos que deben tener controlados y no quiere decir que todos los aspectos que en ella aparecen tienen que ser implementados con los últimos avances. Todo dependerá de la naturaleza de la propia organización. De la relevancia demostrada de la normativa de seguridad se muestra a continuación el cuadro 1 evolución de la normativa.

Cuadro 1
Evolución de la normativa.

Año	Norma
1995	BS 7799-1:1995
1999	BS 7799-2:1999
1999	Revisión BS 7799-1:1999
2000	ISO/IEC 17799:2000
2002	Revisión BS 7799-2:2002
2005	Revisión ISO/IEC 17799:2005
2005	Revisión BS 7799-2:2005
2005	ISO/IEC 27001:2005 (Norma internacional certificable)

Nota: Autor(2.006)

El conjunto de estándares que aportan información de la familia ISO-2700x, que se deben tener en cuenta como marco referencial en materia de seguridad y se muestran en el cuadro 2 a continuación:

Cuadro 2
Futuro de la normativa.

Norma	Descripción	Año de publicación
ISO 27000	Vocabulario y Definiciones	2007
ISO 27001	ISMS-Estándar Certificable (revised BS 7799 Part 2:2005) Publicado el 15 de octubre del 2005	2005
ISO 27002	Código de Buenas Prácticas, relevo de ISO 17799:2005. Publicado el 15 de junio del 2005	2007
ISO 27003	Guía para la Implantación (bajo desarrollo)	2008
ISO 27004	Métricas e Indicadores (bajo desarrollo)	2008
ISO 27005	Gestión de Riesgos (BS 7799-3:2006) (basado e incorporado a ISO/IEC 13335 MICTS Part 2) (bajo desarrollo)	2008
ISO 27006	Continuidad de Negocio / Recuperación Desastres	2007

Nota: Autor(2.006)

Norma ISO/IEC-27001:2005

Según la Norma: El estándar internacional ha sido preparado con la finalidad de proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Este estándar internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización. La organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de insumos en productos, se puede considerar

un proceso. Con frecuencia el producto de un proceso forma directamente el insumo del siguiente proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos y su gestión, puede considerarse un "enfoque del proceso".

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
- Implementar y operar controles para manejar los riesgos de la seguridad de la información;
- Monitorear y revisar el desempeño y la efectividad del SGSI; y
- Mejoramiento continúo en base a la medición del objetivo.

El estándar internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. El Gráfico muestra cómo un SGSI toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. El Gráfico 2 y el cuadro 3 también muestran los vínculos en los procesos presentados en las Cláusulas 4, 5, 6, 7 y 8 de la norma y la descripción del modelo respectivamente.

La adopción del modelo PDCA también reflejará los principios tal como se establecen en los Lineamientos OECD (2.002)[11] que gobiernan los sistemas y redes de seguridad de la información. Este estándar internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que gobiernan la evaluación

[11] Lineamientos OECD para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad. París: OECD, Julio 2002. www.oecd.org.

del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad.

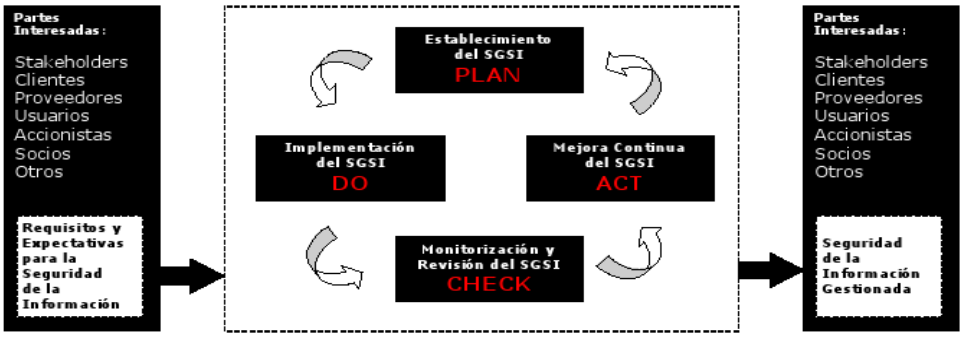


Gráfico 2: Modelo PDCA aplicado a los procesos SGSI. ISO/IEC-27001:2005

Cuadro 3
Descripción del Modelo PDCA aplicado a los procesos SGSI

Planear (establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Chequear (monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Nota: ISO/IEC-27001:2005

Norma ISO/IEC-17799:2005

Este estándar internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este estándar internacional proporcionan un lineamiento sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este estándar internacional son diseñados para ser implementados y satisfacer los requerimientos identificados por una evaluación del riesgo. Este Estándar Internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales.

Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

Las once cláusulas y el número de categorías de seguridad principales incluidas dentro de cada cláusula son:

a) Política de Seguridad (1);
b) Organización de la Seguridad de la Información (2);
c) Gestión de Activos (2);
d) Seguridad de Recursos Humanos (3);
e) Seguridad Física y Ambiental (2);
f) Gestión de Comunicaciones y Operaciones (10);
g) Control de Acceso (7);
h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (6);
i) Gestión de Incidentes de Seguridad de la Información (2);
j) Gestión de la Continuidad Comercial (1);
k) Conformidad (3).

Políticas de Seguridad.

Maiwald (2.005), plantea que la política de seguridad define los requerimientos técnicos para la seguridad en sistemas de cómputo y el equipo de redes. Define la manera en que un administrador de redes o sistemas debería configurar un sistema respecto a la seguridad. Esta configuración también afectará a los usuarios, y algunos de los requerimientos establecidos en la política deberían comunicarse a la comunidad

de usuarios en general. La responsabilidad principal para la implementación de esta política recae sobre los administradores del sistema y de la red, siempre con el respaldo de la administración.

Las políticas proporcionan las reglas que gobiernan cómo deberían ser configurados los sistemas y como deberían actuar los empleados de una organización en circunstancias normales y cómo deberían reaccionar si se presentan circunstancias inusuales. Propiamente dicho, la política realiza dos funciones principales:

- Define lo que debería ser la seguridad dentro de una organización.
- Pone a todos en la misma situación, de modo que todo el mundo entienda lo que se espera de ellos.

Hay tres secciones de cada política que son comunes y que se examinarán como sigue:

- **Propósito:** cada política y procedimiento debería tener un propósito bien definido, que articule claramente por qué fueron creados tal política o procedimiento, y que beneficio espera la organización derivar de los mismos.
- **Ámbito:** Cada política y procedimiento debería tener una sección que defina su aplicabilidad. Por ejemplo, una política de seguridad debe aplicarse a todos los sistemas de cómputo y de redes. Una política de información puede aplicarse a todos los empleados.
- **Responsabilidad:** La sección de responsabilidad de una política o procedimiento define quién se hará responsable por la implementación apropiada del documento. Quienquiera que sea designado como el responsable de aplicar una política o procedimiento debe ser capacitado de manera adecuada y estar consciente de los requerimientos del documento.

Plan de Seguridad

Sanz (2.006) explica que el plan de seguridad es la herramienta utilizada por las empresas para garantizar la seguridad de sus sistemas y servicios. Consiste en una serie de normas, procedimientos y políticas que se implantan en la estructura de una

organización con el objetivo de detectar, corregir y prevenir todos los riesgos de seguridad, tanto presentes como futuros.

La estructura de un Plan de Seguridad se divide en varias fases:

- Identificación de elementos a proteger.
- Análisis y valoración de los riesgos presentes y futuros.
- Diseño de unas medidas de seguridad que eliminen o mitiguen dichos riesgos.
- Implantación de dichas medidas de seguridad.
- Auditoría de las medidas implementadas (repetida de forma periódica).
- Revisión y actualización de las medidas implantadas.

A groso modo, un buen Plan de Seguridad debería contemplar los siguientes aspectos:

- Política de gestión y administración de equipos, elementos de red y servicios; que cubra la instalación, configuración y uso diario seguro de todos los elementos que conforman la red.
- Política de administración de parches y actualizaciones; que mantenga los equipos al nivel de actividad óptimo en cuanto a seguridad y rendimiento.
- Procedimientos de transmisión segura de datos; que garanticen la seguridad de las comunicaciones entre la empresa y clientes o proveedores.
- Normas de seguridad física; que permitan realizar un control de acceso efectivo a las instalaciones en las que se encuentran los elementos que conforman la red.
- Procedimientos de gestión y administración de usuarios y contraseñas; que establezcan un control efectivo y robusto de los accesos y permisos existentes en el sistema.
- Política de antivirus; que permita asegurar que los contenidos ofrecidos están libres de virus, troyanos y cualquier otro elemento pernicioso para el usuario.

- Política de gestión y almacenamiento de logs o registros; que permita realizar un seguimiento de los accesos realizados tanto a los servicios como a los recursos de la empresa.
- Política de copias de seguridad o backups; que permita, ante un fallo catastrófico del sistema, restaurar el mismo con la menor pérdida de datos posible.
- Procedimientos ante contingencias del sistema; que garanticen una actuación rápida y eficaz ante cualquier fallo del servicio.
- Procedimientos ante incidencias de seguridad del sistema; que permitan reaccionar, identificar, actuar y contrarrestar cualquier tipo de acceso no autorizado a los sistemas que prestan el servicio.
- Procedimientos de formación y concienciación del personal de la empresa; con el fin de garantizar el conocimiento de unas prácticas básicas de seguridad.

Es importante reseñar que el Plan de Seguridad es una iniciativa que afecta a todos los estratos de un sistema. Se gesta y efectúa desde el Departamento de Sistemas Informáticos, pero necesita por una parte del apoyo de la Dirección (para que asigne los recursos económicos y humanos necesarios para su ejecución), y por otra parte de todos los usuarios del sistema, que deben estar concienciados y sensibilizados acerca de la importancia de la seguridad en su sistema.

Administración del riesgo

De acuerdo a Maiwald (2.005) la seguridad se consigue administrando el riesgo. Si no se entiende cuales son los riesgos de seguridad para los activos de información de la organización, pueden utilizarse demasiados o escasos recursos, o utilizarlos de manera equivocada. La administración de riesgos también proporciona una base para el avaluo de los activos de información. Al identificar los riesgos, usted puede identificar el valor

de los tipos particulares de información y el valor de los sistemas que contienen esa información.

El riesgo es el potencial de lo que puede ser perdido y requiere protección. El riesgo contiene dos componentes: la amenaza y la vulnerabilidad. De ello se puede inferir que el riesgo es igual a la suma de las amenazas y las vulnerabilidades.

"Riesgo = vulnerabilidad + amenaza".

Se entiende por vulnerabilidad una vía de ataque potencial. Las vulnerabilidades pueden existir en redes y sistemas de computo o en procedimientos administrativos. Una amenaza es una acción o evento que puede violar la seguridad de un entorno de sistemas de información. Existen tres componentes de amenaza:

- Objetivos: El aspecto de la seguridad que puede ser atacado.
- Agentes: Las personas u organizaciones que origina la amenaza.
- Eventos: El tipo de acción que representa la amenaza.

En este sentido CERT[12] (Computer Emergency Response Team), equipo de respuesta de emergencias a incidentes de seguridad creado por DARPA[13] (Defense Advanced Research Projects Agency) en 1.988, publica en su site web el cuadro 4 que muestra las vulnerabilidades reportadas, dando un total de 26.713.

Cuadro 4
Vulnerabilidades divulgadas. 1995-2006

Año	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	Q1-Q2,2006
Vulnerabilidades	171	345	311	262	417	1,090	2,437	4,129	3,784	3,780	5,990	3,997

Nota: www.cert.org

El CERT trabaja para facilitar las respuestas a incidentes de seguridad que afectan a Internet, con el objetivo de tomar las medidas oportunas de prevención, además de investigar y mejorar la seguridad de los sistemas que existen.

[12] CERT: Equipo de Respuesta a Incidentes de Seguridad en Cómputo. www.cert.org
[13] DARPA: La Agencia de Investigación de Proyectos Avanzados de Defensa. http://www.darpa.mil/

Con la finalidad de realizar una administración del riesgo se debe elaborar un análisis de riesgos y tomar como referencia el estándar.

Análisis del Riesgo y los Requerimientos del ISO 27001:2005

Alexander (2.006) expresa: "El ISO 27001:2005 requiere que la organización que esta planeando implantar un SGSI, primero defina el alcance del estándar en la empresa, y en base a ese alcance identifique todos los activos de información."

Para identificar los activos de información se puede utilizar la metodología de las elipses, "la cual una vez determinado el alcance se decide el proceso que se evaluará. Con esto se trata de visualizar con mucha precisión los distintos subprocesos que componen al alcance. Esto se determina en la elipse concéntrica, el paso siguiente sería determinar los usuarios y dueños de esos procesos, el segundo paso en la metodología, es el de identificar en la elipse intermedia las distintas interacciones de los subprocesos de la elipse concéntrica, tienen con otros procesos de la organización. Seguidamente, también se deben identificar con la elipse concéntrica. La elipse externa, se identifican aquellas organizaciones extrínseca a la empresa que tienen cierto tipo de interacción con los subprocesos identificados en la elipse concéntrica."

Los activos de información deben ser tasados para identificar su impacto en la organización. Luego un análisis del riesgo es requerido para determinar que activos están bajo riesgo. "Se deben tomar decisiones en relación a que riesgos la organización aceptará y que controles serán implantados para mitigar el riesgo". A la gerencia se le requiere que revise el SGSI en la organización a intervalos planificados para asegurar su adecuación y eficacia. La gerencia es exigida que controle los niveles de riesgos aceptados y el estado del riesgo residual (riesgo que queda después del tratamiento del riesgo). El ISO 27001:2005 es un sistema dinámico que obliga a la gerencia estar constantemente revisando y definiendo controles, sus amenazas, vulnerabilidades e iniciar acción correctiva y preventiva cuando sea necesario.

Proceso de Evaluación del Riesgo

El proceso de evaluación del riesgo que permite a una organización estar en conformidad con los requerimientos del estándar esta presentada en el gráfico 3. El proceso de las seis (6) fases ayuda a cualquier organización que desee establecer un SGSI, en concordancia con la cláusula 4.2.1 del estándar.

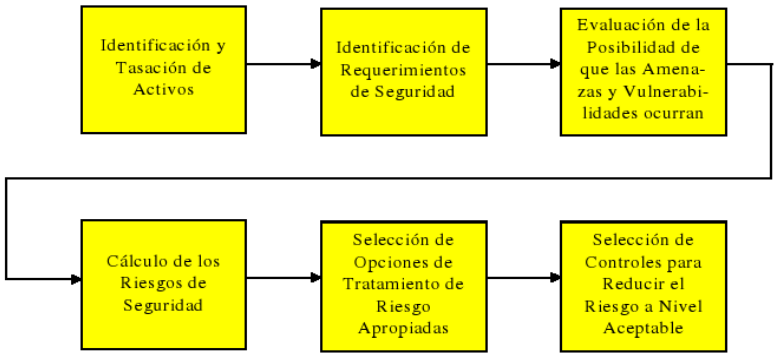


Gráfico 3: Proceso de evaluación de riesgo

Identificación y Tasación de Activos: Un activo es algo que tiene valor o utilidad para la organización, sus operaciones y su continuidad. Los activos necesitan protección para asegurar las correctas operaciones del negocio y la continuidad de la empresa. "La gestión apropiada de los activos es vital para poder mantener una adecuada protección de los activos de la empresa."

Cada activo debe estar claramente identificado y valorado apropiadamente, y su propietario y clasificación de seguridad acordada en la organización. El ISO 17799:2005 (Código de Práctica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera: (1) Activos de información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad; (2) Documentos impresos: contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes del negocio; (3) Activos de software: Software de aplicación, software de sistemas, herramientas de desarrollo; (4) Activos

físicos: Equipos de comunicación y computación, medios magnéticos, otros equipos técnicos; (5) Personas: Personal, clientes, suscriptores; (6) Imagen y reputación de la compañía; (7) Servicios: Servicios de computación y comunicación, otros servicios técnicos.

La tasación de activos, basados en las necesidades del negocio de una organización, es un factor importante en la evaluación del riesgo. Para poder encontrar la protección apropiada para los activos, es necesario evaluar su valor en términos de su importancia para el negocio. "Para poder tasar los valores de los activos y poder relacionarlos apropiadamente, una escala de valor para activos debe ser aplicada."

Identificación de Requerimientos de Seguridad: Los requerimientos de seguridad en cualquier organización, grande o pequeña, son derivados de tres fuentes esenciales y debieran de documentarse en un SGSI.

- El conjunto único de amenazas y vulnerabilidades que pudieran ocasionar pérdidas significativas en la empresa si ocurrieran.
- Los requerimientos contractuales que deben satisfacerse por la organización.
- El conjunto único de principios, objetivos y requerimientos para el procesamiento de información que una organización ha desarrollado para apoyar las operaciones del negocio y sus procesos.

Una vez que estos requerimientos de seguridad han sido identificados, es recomendable formularlos en términos de requerimientos de confidencialidad, integridad y disponibilidad.

Identificación de Amenazas y Vulnerabilidades: Los activos están sujetos a muchos tipos de amenazas. Una amenaza tiene el potencial de causar un incidente no deseado, el cual puede generar daño al sistema, la organización y a los activos. El daño puede ocurrir por un ataque directo o indirecto a la información organizacional. Las amenazas pueden originarse de fuentes accidentales o de manera deliberada. Una amenaza para poder causar daño al activo, tendría que explotar la vulnerabilidad del sistema, aplicación o servicio.

Las vulnerabilidades son debilidades asociadas con los activos organizacionales. Las debilidades pueden ser explotadas por la amenaza, causando incidentes no deseados, que pudieran terminar causando pérdidas, daño o deterioro a los activos. La vulnerabilidad como tal, no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo. Una evaluación de la posibilidad de ocurrencia de las vulnerabilidades y las amenazas, debe ser efectuada en esta fase.

Cálculo de los Riesgos de Seguridad: El objetivo de la evaluación del riesgo es la de identificar y evaluar los riesgos. Los riesgos son calculados de una combinación de valores de activos y niveles de requerimientos de seguridad. La evaluación de riesgos envuelve la sistemática consideración de los siguientes aspectos:

- Consecuencias: El daño al negocio como resultado de un incumplimiento de seguridad de información considerando las potenciales consecuencias de pérdidas o fallas de confidencialidad, integridad y disponibilidad de información.
- Probabilidad: La real posibilidad de que tal incumplimiento ocurra a la luz del reinado de amenazas, vulnerabilidades y controles.

Es importante destacar que no existe una manera "buena" o "mala" de calcular los riesgos, en la medida que los conceptos descritos en las fases anteriores se combinen en una manera sensata. Es menester de la firma identificar un método para la evaluación del riesgo que sea adecuada a los requerimientos de seguridad del negocio.

Selección de Opciones Apropiadas de Tratamiento del Riesgo: Cuando los riesgos han sido identificados y evaluados, la próxima tarea para la organización es identificar y evaluar la acción más apropiada de cómo tratar los riesgos. La decisión debe ser tomada basada en los activos involucrados y sus impactos en el negocio. Otro aspecto importante a considerar es el nivel de riesgo aceptable que ha sido identificado siguiendo la selección de la metodología apropiada de evaluación.

El estándar ISO 27001:2005 requiere que la organización en relación al tratamiento del riesgo siga cuatro posibles acciones:

- Aplicación de apropiados controles para reducir los riesgos. Los controles tienen que ser identificados en el (Anexo "A") . Si los controles no pueden ser hallados, la firma puede crearlos y documentarlos.
- Aceptar objetivamente los riesgos partiendo del supuesto que satisfacen la política de la organización y su criterio para la aceptación del riesgo.
- Evitar los riesgos
- Transferir el riesgo asociado a otras partes.

La organización por cada uno de los riesgos, debe evaluar estas opciones para identificar la más adecuada. Los resultados de esta actividad deben ser documentados y luego la firma debe documentar su "plan de tratamiento del riesgo".

Hay dos opciones en la identificación y evaluación del riesgo que requieren mayor explicación. Las alternativas son: "evitar el riesgo" y "transferencia del riesgo". (a) Evitar el riesgo. Describe cualquier acción donde los activos son transferidos de las áreas riesgosas. Cuando se evalúa la posibilidad de "evitar el riesgo" esto debe sopesarse entre las necesidades de la empresa y las monetarias. (b) Transferencia del riesgo. Esta opción puede ser vista como la mejor si es imposible reducir los niveles del riesgo. Existen muchas alternativas a considerar en relación a la estrategia de transferencia del riesgo. La transferencia del riesgo podría alcanzarse tomándose una póliza de seguro. Otra posibilidad podría ser la utilización de servicios de "outsourcing" para que se manejen activos y procesos críticos. La responsabilidad por los servicios tercerizados siempre recae en la empresa. Eso jamás se delega.

Selección de Controles para Reducir los Riesgos a un Nivel Aceptable: Para reducir el riesgo evaluado dentro del alcance del SGSI considerado, controles de seguridad apropiados y justificados deben ser identificados y seleccionados. Estos controles deben ser seleccionados del estándar ISO 27001:2005 Anexo "A". El estándar presenta once (11) cláusulas, treinta y nueve (39) objetivos de control y ciento treinta y tres (133) controles específicos. Es muy importante estar claros sobre el rol del ISO

17799:2005. ***La organización puede utilizar el ISO 17799:2005 como guía para la implementación de los controles, pero deben ser escogidos del ISO 27001:2005.***

La selección de los controles debe ser sustentada por los resultados de la evaluación del riesgo. Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y que forma debe tener. Especialmente para propósitos de certificación, las relaciones con la evaluación del riesgo deben ser documentadas para justificar la selección de los controles.

Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados, incluyendo:

- Uso de controles
- Transparencia del usuario
- Ayuda otorgada a los usuarios para desempeñar su función
- Relativa fuerza de los controles
- Tipos de funciones desempeñadas.

En términos generales, un control podrá satisfacer más de una de estas funciones y lo más que pueda satisfacer mejor.

Reducción del Riesgo y su Aceptación: Para todos aquellos riesgos donde la decisión de "reducción de riesgo" ha sido escogida, controles apropiados deben ser seleccionados para reducir los riesgos a un nivel que la gerencia hubiese establecido, de acuerdo a la cláusula del estándar 5.1 (f) decidirá su nivel adecuado de la ISO/IEC 27001:2005

Riesgo Residual: Después de identificar los controles adecuados para reducir un riesgo específico al nivel considerado aceptable, debe evaluarse cuanto reducirán el riesgo los controles, si se implementan. Esta reducción de riesgo es el denominado "riesgo residual".

El riesgo residual usualmente es difícil evaluarlo. Por lo menos, una estimación de cuanto los controles reducen el nivel de los requerimientos de los valores asociados

de seguridad debieran ser identificados para asegurar que la suficiente protección es alcanzada.

Si el riesgo residual es inaceptable, una decisión comercial debe ser tomada sobre como se irá a manejar la situación. Una opción es la de seleccionar más controles para finalmente reducir los riesgos a un nivel aceptable. Es una buena práctica no tolerar riesgos inaceptables, pero muchas veces no es posible o financieramente factible reducir todos los riesgos al nivel aceptable.

Después de la implementación de los controles seleccionados, es importante estar claros que siempre habrá riesgos existentes. Esto sucede porque los sistemas de información en las organizaciones nunca podrán estar absolutamente seguros. Esta es la razón por la cual es necesario revisar la implementación, y los resultados de los controles para finalmente evaluar qué tan bien los controles implementados están operando. Este es fundamentalmente el propósito de las "revisiones gerenciales" para poder tener un control concreto del proceso del riesgo en la firma y poder iniciar la acción correctiva cuando sea necesario.

En definitiva y como cierre de las bases teóricas, se puede verificar que las mismas guardan una relación con la investigación en función de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

Bases Legales

Los estándares internacionales, leyes nacionales y normativa interna de la Universidad que tienen correspondencia con esta investigación se listan a continuación:

Estándares Internacionales

ISO/IEC 27001:2005 Sistemas de Gestión de Seguridad de la Información – Requerimientos. Organización Internacional de Estándares (ISO).

ISO/IEC 17799:2005 Código para la Práctica de la Gestión de la Seguridad de la Información Organización Internacional de Estándares (ISO).

Lineamientos OECD para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad.

Leyes Nacionales

Ley Especial Contra Delitos Informáticos promulgada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2.001 por la Asamblea Nacional, Caracas - Venezuela.

Ley Sobre Mensajes de Datos y Firmas Electrónicas promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2.001, por Decreto N° 1.024 – 10 de febrero de 2.001, Caracas - Venezuela.

Ley Orgánica de Telecomunicaciones, promulgada 12 de junio de 2000 y publicada en Gaceta Oficial No.36.970. Caracas - Venezuela.

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 2.004. 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 2.005. Barquisimeto - Venezuela

Sistema de Variables

De acuerdo a lo expresado por Balestrini (1.998), una variable es un aspecto o dimensión de un objeto, o una propiedad de estos aspectos o dimensiones que adquiere distintos valores y por lo tanto varía. La misma autora señala que, en el proceso lógico

de operacionalización de las variables, se han de seguir los siguientes procedimientos: (i). Definición nominal de la variable a medir; (ii). Definición real: enumeración de sus dimensiones y (iii) Definición operacional: selección deindicadores.

La definición nominal se relaciona con el cuerpo teórico en el cual está contenida la hipótesis en cuestión o la variable en estudio. En esta etapa del proceso de operacionalización de las variables, se establece específicamente el significado que ha de otorgarsele a un determinado término dentro de la investigación y tiene la ventaja de proporcionar una mayor precisión en el establecimiento de los objetivos de la investigación.

En el caso de la presente investigación la variable a considerar fue el diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

La definición real está relacionada con el establecimiento de las propiedades (dimensiones) consideradas esenciales del objeto u hecho referido en la investigación. Se trata de descomponer el concepto original en las dimensiones que lo integran. De acuerdo a lo señalado, la dimensión fue: Seguridad de informática

Asimismo, la definición operacional implica seleccionar los indicadores contenidos, de acuerdo al significado que se le ha otorgado a través de sus dimensiones a la variable en estudio, para lo que es necesario definir las variables teóricas en términos de variables empíricas o indicadores, indicando el qué, cuándo y cómo de la variable y las dimensiones que la contienen.

De acuerdo a la definición operacional, para el caso del estudio que se presenta, los indicadores relacionados con seguridad informática serán: 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 Acceso, Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, Gestión de Incidentes de Seguridad de la Información, Gestión de la Continuidad Comercial, Conformidad.

A continuación se presenta el cuadro 5, con la operacionalización de las variables en estudio.

Cuadro 5
Operacionalización de las Variables

Variable en Estudio	Dimensión	Indicadores	Instrumentos	Fuente
Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.	Seguridad informática	○ 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 Acceso. ○ Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. ○ Gestión de Incidentes de Seguridad de la Información. ○ Gestión de la Continuidad Comercial. ○ Conformidad.	○ Entrevistas ○ Cuestionario ○ Observación Directa.	○ Coordinaciones ○ Personal OCTSI

Nota: Autor (2.006)

CAPITULO III

MARCO METODOLOGICO

Naturaleza de la Investigación

"El éxito no se logra sólo con cualidades especiales. Es sobre todo un trabajo de constancia, de método y de organización."
J.P. Sergent

El presente estudio se ubicó en la modalidad de proyecto factible, por ser una investigación desarrollada en el espacio y en el tiempo durante un período determinado, previo análisis y diagnóstico de la situación que se ejecutó, y por cuanto pretendió satisfacer necesidades de tipo institucional, como lo fue el diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral. Tomando como referencia la norma ISO/IEC-27001:2005 y la norma ISO/IEC-17799:2005, las cuales tienen concebido mejoras en la seguridad de sus redes de datos. Según Barrios (2.004), un proyecto factible "consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos". A continuación se detallan las cuatro fases en que se estructuró la investigación.

Diseño de la Investigación

En función del enfoque metodológico que se propone, el proceso de investigación se realizó a través de las cuatro fases fundamentales en la formulación de un proyecto factible: Fase I Diagnóstico; Fase II Factibilidad; Fase III Diseño del Plan de Seguridad

Informática y Fase IV Evaluación del Plan de Seguridad Informática. Esta metodología esta definida en Barrios (2.004), de la siguiente manera:

Fase I Diagnóstico

Comprendió el estudio de la situación que caracteriza la organización en cuanto a la variable en estudio, para lo cual se desarrollaron las primeras etapas de la metodología de análisis de información, a través de la aplicación de técnicas e instrumentos.

Población y Muestra

Desde el punto de vista estadístico, Balestrini (ob.cit.), indica que una población o universo "puede estar referido a cualquier conjunto de elementos de los cuales se pretende 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 señala que para seleccionar la población, es necesario considerar cuál será la unidad de análisis, lo que permitirá definir con qué elementos (personas, organizaciones) se va a trabajar.

En el caso de esta de investigación, la población para diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral, tomando como referencia la norma ISO/IEC-27001:2005 y la norma ISO/IEC-17799:2005, estuvo constituida por el conjunto de empleados de la Universidad que laboran en el área de tecnología y que se detalla a continuación en el cuadro 6.

Cuadro 6
Descripción de la Población

Descripción	Cargo	Cantidad
Gerencia	Director Tecnología	1
	Coordinador Nacional	3
Grupos de trabajos	Profesionales	14
Apoyo Administrativo	Apoyo Administrativo	2
	TOTAL =======>	**20**

Nota: Autor (2.006)

En cuanto a la muestra, se tomó en cuenta lo expresado por Ary (1.996), 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. Es así que los sujetos de estudio de la presente investigación estuvo conformado por el total de veinte (20) personas que laboran en la Oficina Central de Tecnología y Servicios de Información de la UNEXPO.

Técnicas e Instrumentos de Recolección de Datos

En correspondencia con lo expresado por Hernandez y otros (1.996), una técnica es un procedimiento más o menos estandarizado que se ha utilizado con éxito en el ámbito de la ciencia. Asimismo, señala 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.

En función de los objetivos definidos en la investigación, se emplearon una serie de instrumentos y técnicas de recolección de información, orientadas de manera esencial a alcanzar los fines de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

Dada la naturaleza del estudio y en función de los datos que se requirieron, se introdujo la técnica de la observación directa, no participante y sistemática en la

realidad objeto de estudio y se empleó la técnica de encuesta, con el propósito de interrogar a las personas que laboran en la Universidad.

Hernandez y otros (ob.cit.), 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, frecuencia en que se originan los mismos".

A los efectos de recabar la información pertinente de investigación, también se aplicó la técnica de la encuesta, que es reseñada por Balestrini (ob.cit.), como "aquella que media entre las interrogantes del investigador y las opiniones de los informantes, a través de petición expresa del parecer de éstos respecto a preguntas o proposiciones elaboradas sistemáticamente para el fin" (p. 27).

En relación con los instrumentos de recolección de datos, Hernandez y otros (ob.cit.), señala que un cuestionario "está conformado por preguntas preparadas cuidadosamente y relacionadas con los hechos o aspectos que conforman la investigación, así como es aplicado a la muestra a que se extiende el estudio" (p.73).

Por otra parte, para Sabino (1.998), se concibe una entrevista de la siguiente manera: "Consiste en una interacción entre dos personas, una de las cuales (el investigador) formula determinadas preguntas relativas al tema de investigación, mientras la otra (el investigado) proporciona verbalmente o por escrito la información que le es solicitada" (p.146).

Validez del Instrumento

De acuerdo a Balestrini (ob.cit.), es un concepto del cual pueden tenerse diferentes tipos de evidencias relacionadas con el contenido, evidencia relacionada con el criterio y evidencia relacionada 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 este tipo de validez, 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.

Confiabilidad del Instrumento

Hernández y otros (1.996), 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). En tal sentido, la confiabilidad del cuestionario aplicado a los veinte (20) empleados se determinó a través del Coeficiente Alpha de Cronbach, bajo la siguiente formula:

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

Gráfico 4. Formula Coeficiente Alpha de Cronbach

Donde:

N = Es el numero de ítems.
$\sum SI^2$ = Sumatoria de la varianza por ítems.
St^2 = Varianza Total.
Rango de valores entre (0-1).

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 7
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

Nota: Metodología de la Investigación, por Hernández y otros (1.996)

Técnicas de Análisis de los Datos

Los resultados obtenidos se analizaron 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).

Fase II Factibilidad

Según Senn (1.987). " La factibilidad es la posibilidad de que el sistema sea

beneficioso para la organización ". En este sentido, para la investigación fue necesario determinar la factibilidad operativa, técnica y económica.

Factibilidad Operativa

Esta prueba de factibilidad cuestiona, si el sistema trabaja cuando se instale y desarrolle. En este sentido Scott (1.988) " Describe tres (3) cuestionamientos:

- Un nuevo sistema puede ser demasiado complejo para los usuarios de la organización ó los operadores del sistema; si lo es, los usuarios pueden ignorarlos o usarlos de tal forma que cause errores.
- Un nuevo sistema puede hacer que los usuarios se resistan a él, como consecuencia de una técnica de trabajo, miedo a ser desplazado, interés en sistema antiguo u otras razones.
- Un nuevo sistema puede introducir cambios demasiados rápidos para permitir al personal adaptarse a él ó aceptarlo.

Factibilidad Técnica

Evalúa si el equipo y software están disponibles (en el caso del software, si puede desarrollarse) y si tiene las capacidades técnicas requeridas por cada alternativa de diseño que se esté considerando, las interfaces en los sistemas actuales y el nuevo. De igual manera, considera si la organización tiene el personal que posee la experiencia técnica requerida para diseñar, implantar, operar y mantener el sistema propuesto".

Factibilidad Económica

Según Senn (1.987) "Un sistema que puede desarrollarse técnicamente, ser instalado y utilizado, se considera una buena inversión para la empresa, es decir, los beneficios financieros deben igualar ó exceder los costos financieros".

Fase III Diseño del Plan de Seguridad Informática

Una vez identificada la necesidad en la fase de diagnóstico y estudiada la factibilidad de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral, se procedió a la fase de diseño basado en el modelo PDCA (Plan – Do – Check – Act). En este caso se aplicó la primera etapa del modelo detallándola a continuación:

- Plan - Establecimiento SGSI:
    - Inicio del proyecto.
    - Definición del SGSI.
    - Evaluación del riesgo.
    - Tratamiento del riesgo.

Fase IV Evaluación del Diseño del Plan de Seguridad Informática

Luego de realizar el diseño del Plan de Seguridad Informática y como elemento adicional del presente trabajo se procedió a la implantación, operación y evaluación del mismo, en función del ámbito a aplicar tomando como referencia el modelo PDCA, específicamente la segunda y tercera acción "Do-Check" las cuales se detallan a continuación:

- Do – Implantación y Operación:
    - Formación y sensibilización.
    - Implantación del SGSI.
- Check – Evaluación del plan de seguridad.
    - Monitorización SGSI.
    - Revisión del SGSI.

El cuarto proceso del modelo PDCA "Act", no es alcance del presente trabajo de investigación, puede ser aplicado como mejora continua para la universidad y para futuras investigaciones, así como también, el reforzamiento de esta fase IV.

CAPITULO IV

PROPUESTA DEL ESTUDIO

> "No progresas mejorando lo que ya está hecho, sino esforzándote por lograr lo que aun queda por hacer."
>
> ***Khalil Gibran***

En la propuesta del estudio se llevó a cabo lo descrito en el capítulo III a través de las tres primeras fases descritas. Es importante resaltar que el trabajo se circunscribe en el tiempo desde año 2.005 hasta principios del 2.007. En tal sentido, y como requisito de toda planificación se detalla el Gantt en el (Anexo "B") del diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

Fase I: Diagnóstico

La recolección de los datos se hizo mediante la aplicación de dos (2) instrumentos: una (1) entrevista estructurada (Anexo "C"), la cual constó de dieciséis (16) preguntas abiertas y un cuestionario estructurado (Anexo "D") el cual constó de diez (10) ítems cerrados para medir actitudes y opiniones con el método de escalamiento tipo Likert, según Hernandez y otros (1.996) "consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios ante los cuales se pide la reacción del sujeto a los que se les administra, es decir, se presenta cada afirmación y se pide al sujeto que externe su reacción eligiendo uno de los cinco puntos de la escala. A cada punto se le asigna un valor numérico y al final se obtiene su puntuación total sumando las puntuaciones obtenidas en relación a todas las afirmaciones.". Finalmente se detalla la situación

presentada a través de la observación directa, no participante y sistemática.

Validez y confiabilidad de los instrumentos

En este sentido y con el fin de evaluar los ajustes requeridos para validar el contenido de los instrumentos utilizados, se siguió el procedimiento sugerido, es decir, se sometió a la validez de criterios por juicio de expertos a través del formato para la validación del instrumento (Anexo "E"). Para efectos de la confiabilidad del instrumento "cuestionario" se aplicó una prueba piloto a una muestra seleccionada al azar de cinco (5) personas que laboran en la UNEXPO Vice-Rectorado de Luis Caballero Mejias en Caracas en el área de tecnología, esto con el fin de no contaminar la población objeto de estudio. A los resultados obtenidos de la aplicación del cuestionario se le aplicó el cálculo del coeficiente de confiabilidad Alpha de Cronbach. Una vez realizado los cálculos pertinentes a los valores correspondientes se obtuvo un Alpha = 85,86% (Anexo "F"), esto se traduce en que el instrumento es de "Fuerte confiabilidad" según se establece en cuadro 7 de la presente investigación (ver pág. 44).

Técnica de Análisis y Presentación de los Resultados

Las técnicas que se utilizaron para la obtención de información referente a la investigación fueron las siguientes:

- Aplicación de una entrevista al Coordinador Nacional de Producción y Operaciones quien es el encargado del proceso concerniente a la seguridad de información.
- Aplicación de un "cuestionario" al personal de tecnología y servicios de información que labora en la oficina central adscrita al rectorado.
- Observación directa de la situación presentada en lo referente a seguridad de información, realizada por el investigador.

Resultados de la Entrevista

La entrevista (Anexo "C") fue aplicada al Coordinador Nacional de Producción y Operaciones de la Universidad, esto con el fin de corroborar el estado de la seguridad informática, en este sentido, se obtuvieron como resultado las siguientes respuestas para cada una de las preguntas analizadas en el cuadro 8:

Cuadro 8
Matriz de Registro de la entrevista

Pregunta	Respuesta Obtenida	Análisis
1. ¿Indique si la Universidad está certificada en alguno de los estándares de seguridad de información e indicar de ser afirmativo el estándar, fecha de certificación y entidad certificadora?	No se tiene certificación.	En este ítem se evidencia la no existencia de certificación en seguridad por parte de la universidad.
2. ¿Conoce usted alguno de los estándares de seguridad de información y de ser afirmativo mencione como adquirió usted este conocimiento?	Si, he leído al respecto, pero con exactitud no recuerdo en estos momentos.	Es imprescindible que el personal que labora en el área de tecnología, especialmente la gerencia tenga conocimientos del área de seguridad, esto con la finalidad de lograr comprender todas las acciones que deben establecerse en un plan de seguridad de información.
3. ¿Indique las clasificaciones de seguridad de información actualmente existentes en la Universidad?	No se tiene clasificada la información en la universidad.	Un elemento indispensable para establecer confidencialidad es tener clara la clasificación de seguridad para el tratamiento de la información.
4. ¿Indique el uso que se le da a la información según las clasificaciones existentes en la institución?	No se tiene identificado el uso que se le da a la información.	El uso de la información dentro de cualquier institución debe estar claramente definido a fin de lograr establecer responsables de la misma "propietario".
5. ¿Indique si la institución posee programas dirigidos a sensibilizar sobre la seguridad de la información para todos los empleados?	No se tiene	Un programa de sensibilización a los empleados es factor preponderante para el éxito de la implementación de un plan de seguridad de información.

Pregunta	Respuesta Obtenida	Análisis
6. ¿Las políticas de seguridad son para toda la institución o solo para la dirección de tecnología?	Se tiene cosas básicas, no documentadas, aplicadas a todo el rectorado.	Las políticas de seguridad deben estar documentadas y ser de conocimiento de los empleados que sean afectados por estas políticas.
7. ¿Existe un documento que reúne todas las políticas de seguridad de información vigentes?	No se tiene.	El consolidar toda la información referente a políticas de seguridad, representa un elemento de control dentro del funcionamiento de la seguridad de información.
8. ¿Existe un procedimiento para actualizar periódicamente el documento de políticas de seguridad?	No	Las políticas no son estáticas y por ente requieren de ser revisadas y actualizadas con cierta periodicidad, a fin de estar preparados para los cambios ocurridos en el ambiente.
9. ¿Existe un archivo de Seguridad de Información que reúne todos los convenios vigentes en este sentido?	No	Cuando existe tratamiento con proveedores, agentes externos u otros, se debe tener por escrito el alcance, las responsabilidades y el compromiso de confidencialidad entre las partes.
10. ¿En su institución el plan de continuidad de operaciones cuando se definió o actualizó por última vez, indique si hizo algún simulacro en los últimos seis meses y cuales recomendaron en dicha oportunidad acciones urgentes a realizar para reducir riesgos?	No se tiene.	Establece el plan de recuperación de los procesos de negocio, a veces incluyendo procesos manuales alternativos, el cual forma parte del plan de continuidad del negocio "Business Continuity Plan".
11. ¿En la institución indique cual es el plan de recuperación ante desastres que se tiene y si hizo algún simulacro en los últimos seis meses e indique cuales recomendaciones se realizaron en dicha oportunidad para reducir el riesgos?	No se tiene	Establece la estrategia de recuperación de las aplicaciones críticas. Forma parte del plan de continuidad del negocio "Business Continuity Plan".
12. ¿En la institución han realizado en alguna oportunidad una evaluación de riesgos de la información?	No	El análisis de riesgos del negocio en lo relativo a los sistemas de información es la piedra angular sobre la que se apoyan las acciones para la selección de controles a aplicar e incluso la base para elaborar

Pregunta	Respuesta Obtenida	Análisis
		planes directores o parciales de seguridad, el plan de continuidad del negocio y el plan de seguridad de la información.
13. ¿En la institución han realizado una evaluación de vulnerabilidades de la red y de ser afirmativo ha sido en los últimos seis meses?.	No	Una vulnerabilidad es una debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. El realizar esta evaluación permite tomar medidas para minimizar estas amenazas.
14. ¿En la institución han realizado pruebas de penetración perimetral y de ser afirmativo se recomendaron en dicha oportunidad acciones urgentes a realizar para reducir riesgos?	No se ha realizado	La pruebas de penetración es un método de auditoría mediante el cual se evalúa la seguridad de los sistemas de protección perimetral de una empresa así como los diferentes sistemas que están accesibles desde Internet (routers exteriores, firewall, servidores web, de correo, de noticias, etc), intentando penetrar en ellos y de esta forma alcanzar zonas de la red de una empresa como puede ser la red interna o la DMZ. Este elemento aporta información sobre las posibles vulnerabilidades de seguridad de la organización.
15. ¿En su institución tienen software antivirus y de ser afirmativo indique la fecha de su última actualización.?	Si, se tiene por estaciones de trabajo	Este elemento es importante a fin de evitar daños en la información o procesos.
16. ¿En su institución tienen software para detección de intrusos?	No.	Se debe analizar los resultados obtenidos de los Sistemas de Detección de Intrusos con la finalidad de estudiar su reacción al recibir múltiples y variados ataques. Este aporta indicadores a la hora de establecer registros para la búsqueda de huellas de ataques, a fin de tomar los correctivos necesarios.

Nota: Autor (2006)

Resultados del cuestionario

Seguidamente se presenta los resultados de la aplicación del cuestionario dirigido a los miembros del personal del área de tecnología, específicamente los adscritos al Rectorado, ya que son los casos objetos de estudio, a continuación se establece los acrónimos de las categorías de respuestas:

TD: Totalmente en Desacuerdo
ED: En Desacuerdo
IND: Indeciso
DA: De Acuerdo
TA: Totalmente de Acuerdo

Según lo establecido por escalamiento líkert el valor uno (1) es asignado a TD (Totalmente en Desacuerdo) y el máximo valor de cinco (5) a TA (Totalmente de Acuerdo). El resumen de casos se detalla en el (Anexo "G"), y la tabla de frecuencia para cada una de las preguntas del cuestionario se presenta en el (Anexo "H").

A continuación se realiza el respectivo cuadro de frecuencia, gráfico representativo y el detalle de lo observado estadísticamente tabulado.

Cuadro 9
Certificación de Seguridad Informática

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
1	¿Considera usted que la Universidad tiene certificación en alguno de los estándares de seguridad de información?	9	45	8	40	2	10	1	5	-	-

Nota: Autor (2006)

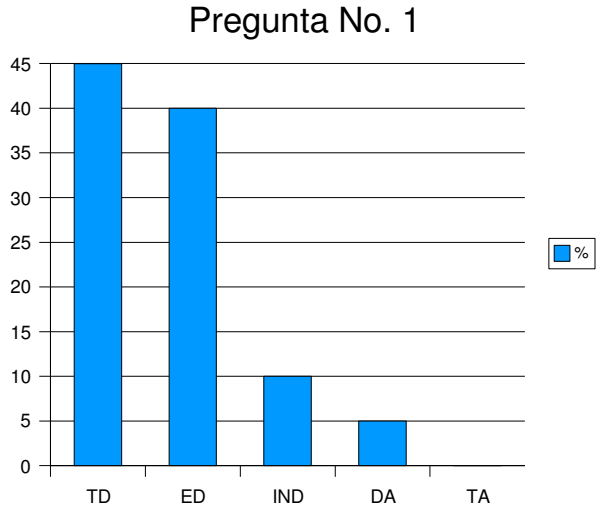


Gráfico 5. Certificación de Seguridad Informática.
Nota: Resultado del análisis y cálculos del instrumento aplicado

Se observa en el gráfico 5 que el ochenta y cinco por ciento (85%) del personal de tecnología considera de que la Universidad no tiene certificación en seguridad de información. Es de notar que una certificación de esta categoría es de conocimiento público en caso de existir.

Cuadro 10
Conocimientos de Seguridad Informática

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
2	¿Tiene usted buenos conocimientos de los estándares de seguridad de información?	2	10	12	60	-	-	6	30	-	-

Nota: Autor (2006)

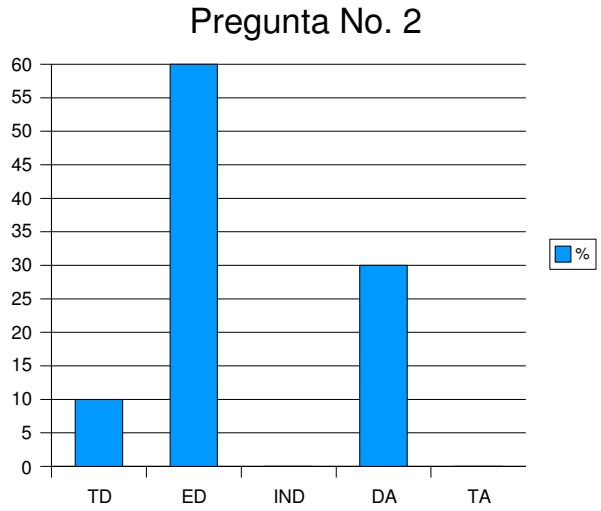


Gráfico 6. Conocimientos de Seguridad Informática.
Nota: Resultado del análisis y cálculos del instrumento aplicado

En el gráfico número 6, el personal de tecnología manifestó claramente en un setenta por ciento (70%), que sus conocimientos sobre los estándares de seguridad no son buenos, solo un treinta por ciento (30%) indicó estar de acuerdo con poseer buenos conocimientos. En este punto se puede inferir la necesidad de adiestrar al personal en esta área y tomar como piloto a aquellos que poseen cierto conocimiento a los efectos de que sirvan como agentes multiplicadores dentro de la organización.

Cuadro 11
Documento de Seguridad Informática

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
3	¿Conoce usted bien el documento de clasificaciones establecidas para la seguridad de la información en la Universidad?	8	40	8	40	2	10	2	10	-	-

Nota: Autor (2006)

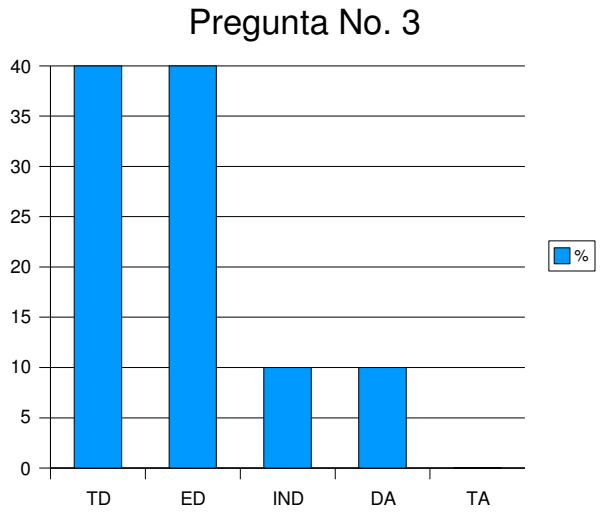


Gráfico 7. Documento de Seguridad Informática.
Nota: Resultado del análisis y cálculos del instrumento aplicado

Se observa en el gráfico 7 una clara tendencia del ochenta por ciento (80%), la cual expresa no conocer la clasificación de la documentación utilizada dentro de la Universidad, hecho relevante a la hora de colocar responsabilidades por uso indebido en el tratamiento de información confidencial.

Cuadro 12
Propiedad de la información

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
4	¿Usted tiene claramente definida y establecida la propiedad de la información de acuerdo a lo asignado por la Universidad?	5	25	8	40	2	10	4	20	1	5

Nota: Autor (2006)

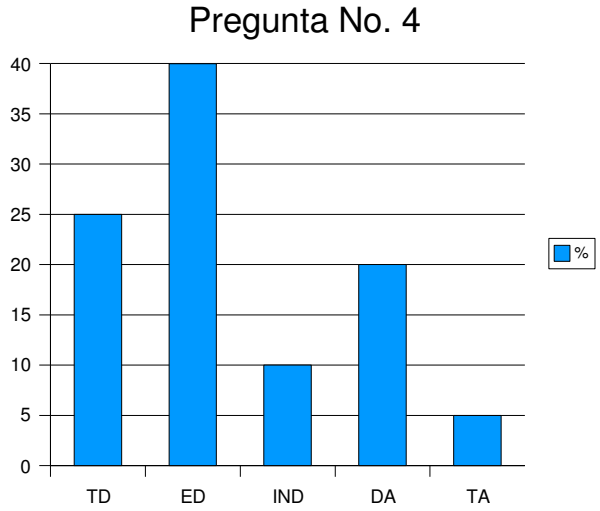


Gráfico 8. Propiedad de la información
Nota: Resultado del análisis y cálculos del instrumento aplicado

Se observa en el gráfico 8 una dispersión en cuanto a la claridad de propiedad de información. Un sesenta y cinco por ciento (65%) no tiene conocimientos sobre su responsabilidad sobre la propiedad de la información, seguido de un veinticinco por ciento (25%) que manifiesta conocer y por último un diez por ciento (10%) que no tiene certeza. Esto puede conducir a inferir que no existe una política clara sobre la propiedad de la información, la cual es fundamental para el tratamiento de la información dentro de una organización que pretende garantizar seguridad de la información.

Cuadro 13
Programas de sensibilización en Seguridad Informática

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
5	¿Sabe con exactitud sobre los programas para sensibilización de seguridad de la información a dictar a todos los empleados?	8	40	11	55	-	-	1	5	-	-

Nota: Autor (2006)

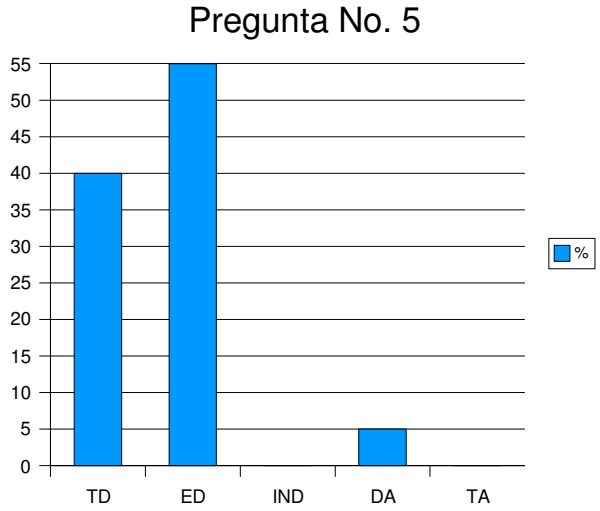


Gráfico 9. Programas de sensibilización en Seguridad Informática
Nota: Resultado del análisis y cálculos del instrumento aplicado

El gráfico 9, muestra una clara tendencia del noventa y cinco por ciento (95%) de los encuestados que manifiestan no tener conocimiento de los programas de sensibilización en seguridad informática. Este ítem es relevante a la hora de establecer un Plan de Seguridad Informática, ya que se debe instruir y sensibilizar a la comunidad que forma vida en la organización.

Cuadro 14
Políticas de Seguridad Informática

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
6	¿Tiene claras las políticas de seguridad de la información de la institución?	6	30	8	40	2	10	4	20	-	-

Nota: Autor (2006)

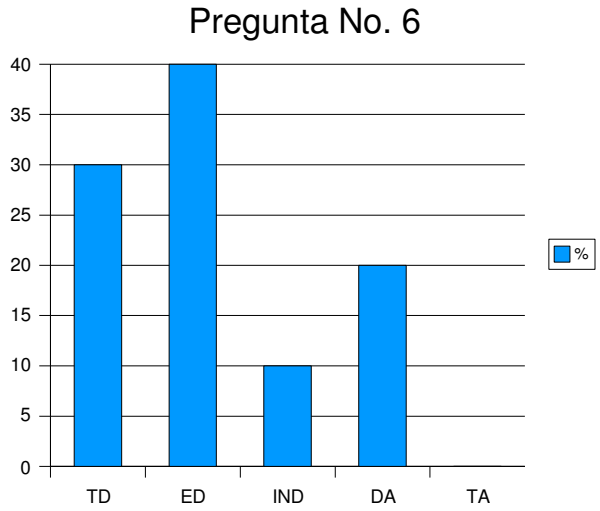


Gráfico 10. Políticas de Seguridad Informática
Nota: Resultado del análisis y cálculos del instrumento aplicado

Se observa en el gráfico 10 un claro desconocimiento sobre las políticas de seguridad de la información por el orden del setenta por ciento (70%), con solo un veinte por ciento (20%) de los encuestados que manifiesta tener conocimiento sobre estas. Se puede inferir de los presentes resultados que las políticas de seguridad informática no tienen el grado de difusión requerido, esto en el caso de que existan, hecho relevante para el plan de seguridad informático.

Cuadro 15
Plan de continuidad de operaciones

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
7	¿Tiene claro el plan de continuidad de operaciones de la institución?	7	35	6	30	3	15	3	15	1	5

Nota: Autor (2006)

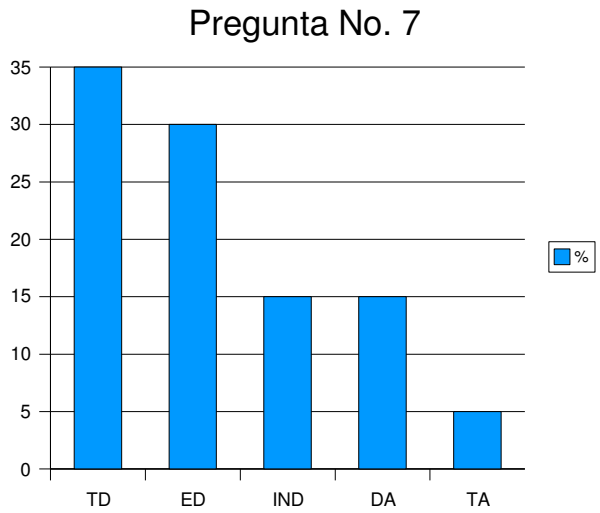


Gráfico 11. Plan de continuidad de operaciones
Nota: Resultado del análisis y cálculos del instrumento aplicado

El gráfico 11 muestra una clara dispersión en lo que respecta al plan de continuidad de operaciones, siendo el porcentaje más representativo un sesenta y cinco por ciento (65%) correspondiente a que no se tiene claridad del Plan, seguido de un veinte por ciento (20%) que dice conocerlo con claridad y un quince por ciento (15%) indeciso.

Cuadro 16
Plan de recuperación ante desastres

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
8	¿En su institución tienen plan eficiente de recuperación ante desastres ?	6	30	9	45	3	15	2	10	-	-

Nota: Autor (2006)

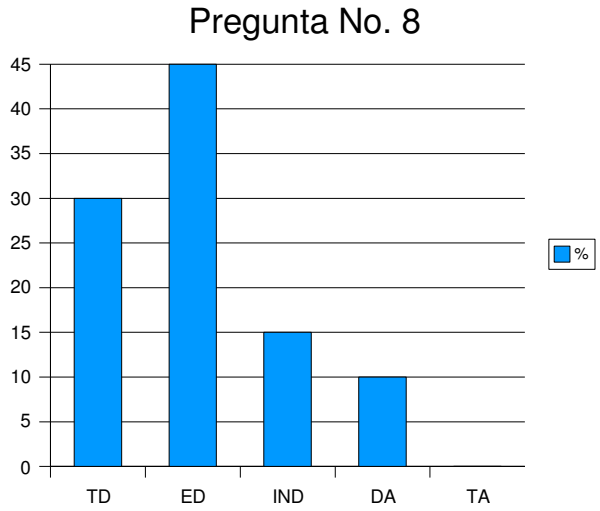


Gráfico 12. Plan de recuperación ante desastres
Nota: Resultado del análisis y cálculos del instrumento aplicado

Se observa en el gráfico 12, una tendencia clara de que el personal de tecnología no está preparado con un plan de recuperación ante desastres, siendo el porcentaje más representativo el setenta y cinco por ciento (75%) representados por el personal que no conoce este plan. Esto da indicios de una clara falta de documentación y difusión de los planes para recuperar la operación de la organización ante elementos considerados como desastres, ej. incendios, terremotos, etc.

Cuadro 17
Evaluación de riesgos

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
9	¿Considera usted que en la institución se han realizado con éxito una evaluación de riesgos de la información?	7	35	7	35	6	30	-	-	-	-

Nota: Autor (2006)

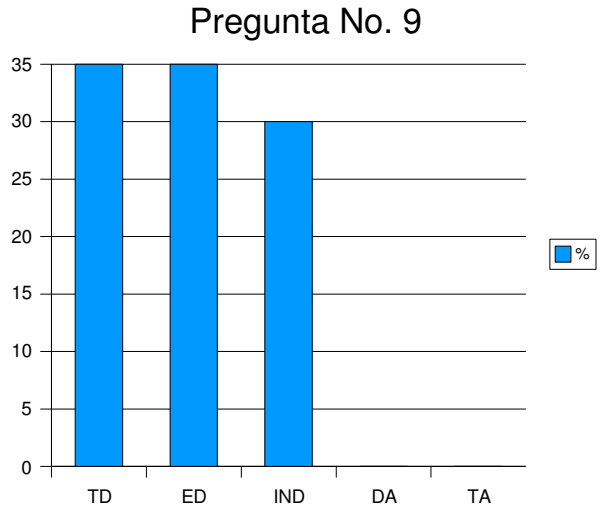


Gráfico 13. Evaluación de riesgos
Nota: Resultado del análisis y cálculos del instrumento aplicado

Se observa en el gráfico 13, una tendencia clara de que el personal de tecnología no ha participado en una evaluación de riesgos, ya que la totalidad indica no tener conocimiento de que exista algún estudio. Elemento primordial para la elaboración de un plan de seguridad de información dentro de cualquier organización.

Cuadro 18
Riesgo de virus

Ítems		Categoría de Respuestas									
		TD	%	ED	%	IND	%	DA	%	TA	%
10	¿Considera que el riesgo de virus en la institución es alto?	2	10	6	30	2	10	6	30	4	20

Nota: Autor (2006)

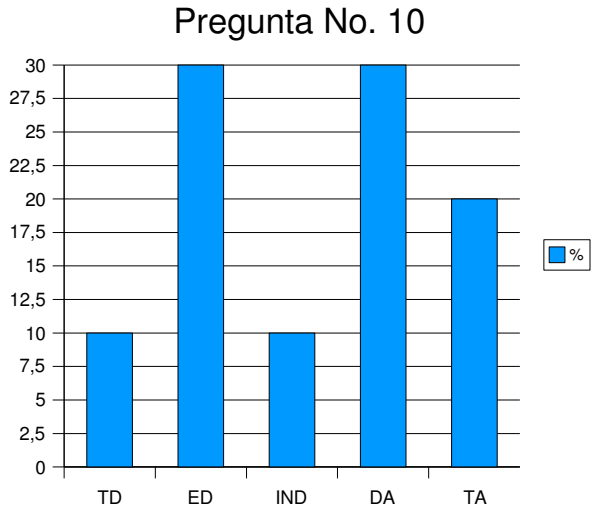


Gráfico 14. Riesgo de virus
Nota: Resultado del análisis y cálculos del instrumento aplicado

El gráfico 14 evidencia una clara división y dispersión en las opiniones del personal de tecnología siendo un cincuenta por ciento (50%) los que opinan tener riesgo de virus, seguido por un cuarenta por ciento (40%) que opina tener minimizada esta posibilidad.

De los resultados obtenidos a través del cuestionario aplicada se pudo observar lo siguiente:

- La universidad no posee certificación bajo estándares de seguridad de información, ya que esto es un hecho de conocimiento público y notorio.
- Existe setenta por ciento (70%) del personal de tecnología que no posee solidos conocimientos sobre seguridad de información y sus estándares.
- El ochenta por ciento (80%) del personal encuestado no tiene conocimiento de como se clasifica la información en cuanto a seguridad dentro de la institución.
- Existe un sesenta y cinco por ciento (65%) del personal que desconoce la propiedad de la información dentro de la institución.
- Un contundente noventa y cinco por ciento (95%) , reconoce la no existencia de planes de sensibilidad en seguridad de la información dentro de la Universidad.
- El setenta por ciento (70%) desconoce las políticas de seguridad de información, elemento clave dentro de todo plan de seguridad.
- Un sesenta y cinco por ciento (65%) manifestó que no conocen el plan de continuidad de operaciones
- El setenta y cinco por ciento (75%) del personal de tecnología no conoce, de existir, el plan recuperación ante desastres.
- Todo el personal, un cien por ciento (100%) manifiesta desconocer si existe un análisis de riesgo sobre los activos de información de la Universidad.
- El riesgo de virus dentro de la institución es contemplado desde el punto de vista del personal de tecnología bajo opiniones divididas, predominando un cincuenta por ciento (50%) que considera que existe riesgo ante esta situación.

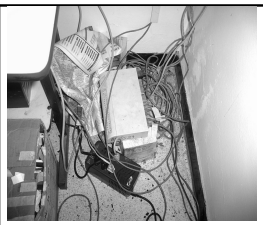
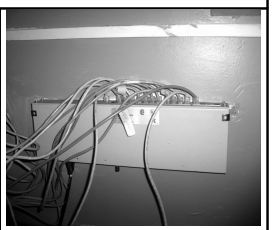
Observación directa

En este ítem se desarrolló lo correspondiente a la observación directa, no participante y sistemática en la realidad objeto de estudio, tomando como guía la norma ISO/IEC-27001:2005, en su apartado "Tabla A.1 Objetivos de control y controles" expresa lo siguiente: "...se derivan directamente de, y se alinean con, aquellos enumerados en BS ISO/IEC 17799:2005 Cláusulas del 5 al 15. Las listas en estas tablas no son exhaustivas..." , en este sentido, se procedió en el cuadro 19 a realizar la observación directa a todos los objetivos de control, tomando como referencia el número uno de cada objetivo.

Cuadro 19
Objetivos de control y controles

A.5 Política de seguridad		
A.5.1 Política de seguridad de información Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.5.1.1	Documentar política de seguridad de información	**Observación Directa:** No existe el documento de políticas, hecho corroborable en la entrevista y el cuestionario.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo*:* Manejar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	**Observación Directa:** Aprobación de los lineamiento y el reglamento de tecnología y servicios de información por Consejo Universitario
A.6.2 Entidades externas Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	**Observación Directa:** No existe análisis de riesgo, hecho corroborable en la entrevista y el cuestionario.
A.7 Gestión de activos		
A.7.1 ***Responsabilidad por los activos*** Objetivo*:* Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	**Observación Directa:** No existe documentación de inventarios de servicios de información, ni tampoco de hardware

A.7.2 Clasificación de la información Objetivo: Asegurar que a información reciba un nivel de protección apropiado.		
A.7.2.1	Lineamientos de clasificación	**Observación Directa:** No existe lineamientos de clasificación, hecho corroborable en la entrevista el cuestionario
A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo Objetivo*:* Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	**Observación Directa:** No existe roles y responsabilidades establecido, hecho corroborable en la entrevista y el cuestionario.
A.8.2 ***Durante el empleo*** Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	**Observación Directa:** No existe gestión de responsabilidades, hecho corroborable en la entrevista y el cuestionario.
A.8.3 Terminación o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	**Observación Directa:** No están definida y asigna claramente las responsabilidades para realizar la terminación o cambio del empleo.
A.9 Seguridad física y ambiental		
A.9.1 ***Áreas seguras*** Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	**Observación Directa:** No existe perímetro de seguridad física para los servicios susceptibles, el Cuarto de Cableado Principal y Servidores (CCPS) se encuentra apagado, sin servidores en producción, el router principal no esta en el CCPS, se violentan todas las normas de cableado estructurado, no hay cableado certificado, existen cascadas de concentradores hasta de 5 niveles. Hecho documentado fotográficamente a continuación:

			
Foto No. 1. Tanquilla sin tapa a la intemperie.	Foto No. 2. Cableado sin canalización	Foto No. 3. Cable sin canalización y concentrador sin rack	Foto No. 4. Cable sin canalización y concentrador sin rack

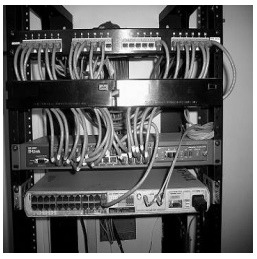
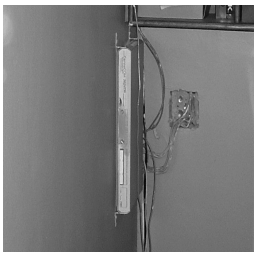
			

Foto No. 5. Cable sin rack descubierto y una Fibra óptica a 10 Mbps en cascada en concentrador	Foto No. 6. Servidor Administrativo, sin respaldo y expuesto.	Foto No. 7. Servidor proxy, expuesto.	Foto No. 8. concentrador de difícil acceso "detrás de unos archivos" y sin rack

A.9.2 *Seguridad del equipo*		
Objetivo*:* Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección del equipo	**Observación Directa:** No existe ver A.9.1.1
A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operacionales		
Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	**Observación Directa:** No existen normas y procedimientos.
A.10.2 Gestión de la entrega del servicio de terceros		
Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.		
A.10.2.1	Entrega del servicio	**Observación Directa:** No existe documentación que asegure que los terceros implementen, operen y mantengan los controles de seguridad.
A.10.3 Planeación y aceptación del sistema		
Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	**Observación Directa:** No existe monitoreo, para realizar proyecciones del uso de los recursos para asegurar el desempeño de los sistemas.
A.10.4 *Protección contra software malicioso y código móvil*		
Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	**Observación Directa:** Existe antivirus en las estaciones de trabajo, sin embargo la actualizaciones las realiza una persona actualizando mediante un diskette cada estación de trabajo.
A.10.5 Respaldo (back-up)		
Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1	*Back-up o respaldo de la información*	**Observación Directa:** No existen.
A.10.6 *Gestión de seguridad de redes*		
Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	**Observación Directa:** No existen.

A.10.7 Gestión de medios Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	**Observación Directa:** No existen.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas de información y software	**Observación Directa:** No existen.
A.10.9 Servicios de comercio electrónico Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		
A.10.9.1	Comercio electrónico	**Observación Directa:** No existen.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	*Registro de auditoría*	**Observación Directa:** No existen.
A.11 Control de acceso		
A.11.1 Requerimiento comercial para el control del acceso Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	**Observación Directa:** No existen.
A.11.2 Gestión del acceso del usuario Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.		
A.11.2.1	Inscripción del usuario	**Observación Directa:** No existen.
A.11.3 Responsabilidades del usuario Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		
A.11.3.1	Uso de clave	**Observación Directa:** No existen.
A.11.4 Control de acceso a redes Objetivo: Evitar el acceso no-autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	**Observación Directa:** No existen.
A.11.5 Control de acceso al sistema de operación Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	**Observación Directa:** No existen.
A.11.6 Control de acceso a la aplicación e información Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
A.11.6.1	Restricción al acceso a la información	**Observación Directa:** No existen.
A.11.7 Computación móvil y tele-trabajo Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.		
A.11.7.1	Computación móvil y comunicaciones	**Observación Directa:** No existen.

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.12.1 Requerimientos de seguridad de los sistemas Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	**Observación Directa:** No existen.
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de data de Insumo	**Observación Directa:** No existen.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	**Observación Directa:** No existen.
A.12.4 Seguridad de los archivos del sistema Objetivo: Garantizar la seguridad de los archivos del sistema		
A.12.4.1	Control de software operacional	**Observación Directa:** No existen.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo*:* Mantener la seguridad del software e información del sistema de aplicación		
A.12.5.1	Procedimientos de control de cambio	**Observación Directa:** No existen.
A.12.6 Gestión de vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	**Observación Directa:** No existen, hecho corroborable en la entrevista y el cuestionario.
A. 13 Gestión de incidentes en la seguridad de la información		
A.13.1 Reporte de eventos y debilidades en la seguridad de la información Objetivo*:* Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
A.13.1.1	Reporte de eventos en la seguridad de la información	**Observación Directa:** No existen.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	**Observación Directa:** No existen, hecho corroborable en la entrevista y el cuestionario.
A.14 Gestión de la continuidad comercial		
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de continuidad	**Observación Directa:** No existen, hecho corroborable en la entrevista y el cuestionario.

	comercial	
A.15 Cumplimiento		
A.15.1 Cumplimiento con requerimientos legales Objetivo*:* Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
A.15.1.1	Identificación de legislación aplicable	**Observación Directa:** No existen.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.		
A.15.2.1	*Cumplimiento con las políticas y estándares de seguridad*	**Observación Directa:** No existen.
A.15.3 Consideraciones de auditoría de los sistema de información Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoría de los sistema de información.		
A.15.3.1	Controles de auditoría de sistemas de información	**Observación Directa:** No existen.

Nota: Autor (2006)

Cada uno de los ítems analizados en la entrevista, el cuestionario y la observación directa, validan lo indicado en el planteamiento del problema y ratifican la necesidad de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

Fase II: Factibilidad

La recolección de datos de la investigación para examinar la factibilidad del proyecto de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral, tiene dentro de sus objetivos 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 el éxito del desarrollo de la investigación 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/05-E09-05.pdf".
- Cada una de las coordinaciones nacionales elaboraron normas y procedimientos de sus respectivas áreas.
- Se llevaron a cabo reuniones con el personal de tecnología para ejecutar la fase de diagnóstico.
- Se realizaron mesas de trabajo con el personal de tecnología para ejecutar los cambios necesarios en cuanto a la infraestructura, así como también para el análisis de riesgo de los activos de información.
- Se envió personal a cursos en el área de seguridad de la información.
- Se impartió adiestramiento a los usuarios finales, respecto a normas básicas de seguridad de información y al nuevo reglamento de Tecnología.

Factibilidad Técnica

El análisis de factibilidad técnica evalúa si el equipo y software están disponibles, y si tienen las capacidades técnicas requeridas por cada alternativa del diseño que se esté considerando. Los estudios de factibilidad técnica también consideran si la organización tiene el personal que posee la experiencia técnica requerida para diseñar, implantar, operar y mantener el diseño propuesto.

En este sentido como se evidenció en la fase de diagnóstico que la Universidad y en especial el rectorado, no posee suficiente personal adiestrado en el área de seguridad, el software que se maneja en la institución son aplicaciones que no están

documentadas, ni certificadas y en lo referente a hardware la infraestructura de red se encuentra fuera de norma, por tanto fue necesario establecer medidas urgentes para la recuperación de un mínimo de control en lo que respecta a seguridad, hecho reflejado en los cuadros 20, 21y 22

Cuadro 20
Garantía Funcional Fase I

Proyecto:	Garantía Funcional Fase I (2.006-2007)
Participación:	Creador del documento. Gerente del proyecto.
Costo:	206.304.100 Bs.
Propósito:	● Garantizar la funcionalidad de los equipos y sistemas. ● Preservar la operatividad y vida útil de los equipos. ● Administrar el servicio de información a través de los esquemas y estándares definidos en la UNEXPO. ● Dotar a la Oficina Central de Tecnología y Servicios de Información de una herramienta de seguimiento y de gestión para la toma de decisiones de tipo técnico. ● Dotar a la UNEXPO de un área que cumpla con todas las normas, estándares y aspecto legales que garanticen la funcionalidad de todos los sistemas y equipos y permita el crecimiento a futuro de la UNEXPO en materia de tecnología y sistemas de información. ● Dotar a la UNEXPO de medios alternativos o redundantes de comunicación a Internet. ● Dotar a la UNEXPO de una plataforma tecnológica actualizada, con capacidad de proceso, integrada, segura, auditable y administrable.
Alcance:	Se acondicionará un área fuera de la sede UNEXPO que garantice la funcionalidad cumpliendo todas las normas, estándares y aspectos legales, tomando en cuenta los inconveniente que se puedan presentar por disturbios o eventos que imposibiliten el acceso a la UNEXPO, por tanto, está área fuera de la sede dará garantía de funcionamiento. Todos los aspectos físicos y ambientales tales como, estructura física, sistema eléctrico, sistema aire acondicionado, humedad, interferencias eléctricas, sistemas de seguridad contra incendio, vigilancia, normas, estándares y aspectos legales son tomados en cuenta. Los sistemas de respaldo de Software y Hardware serán implantados con tecnología de punta y redundancia que garanticen la funcionalidad. Se colocará enlaces redundantes de conexión a internet para garantizar las comunicaciones. Esto se encuentra en trámites de licitación con el nombre de "Contratación de la prestación del servicio de telecomunicaciones entre las sedes principales de la UNEXPO, incluyendo transporte de voz, vídeo, datos y el servicio de Internet"

Nota: Autor (2006).

Cuadro 21
Normalización de Plataforma en las Estaciones de Trabajo

Proyecto:	Normalización de Plataforma en las Estaciones de Trabajo (2.005-2006)
Participación:	Grupo Plataforma tecnológicas Grupo Seguridad y Auditoría
Costo:	107.497.082,18 Bs.
Propósito:	● Dotar a la institución de un servicio de información con tecnología de punta, para que se puedan realizar operaciones en cuanto a soporte técnico se refiere de modo integrado y eficiente. ● Proveer de una herramienta adecuada de control para la OCTSI para las auditorías correspondientes tanto del personal técnico como de los equipos de computación. ● Dotar a la Oficina Central de Tecnología y Servicios de Información (OCTSI) de una herramienta de seguimiento y de gestión para la toma de decisiones del tipo técnica. ● Administrar el servicio de información a través de los esquemas y estándares definidos en la UNEXPO.
Alcance:	● Políticas de seguridad en las estaciones de trabajos. ● Normas y estándares en cuanto a la configuración de las estaciones de trabajo. ● Procedimientos de trabajo para el personal técnico. ● Plataformas tecnológica actualizada, con capacidad de proceso, integrada, segura, auditable y administrable.

Nota: Autor (2006).

Cuadro 22
Rediseño y Actualización de la Infraestructura de Red del Rectorado

Proyecto:	Rediseño y Actualización de la Infraestructura de Red del Rectorado (2.005-2006)
Participación:	Creador del documento. Gerente del proyecto.
Costo:	323.003.967,29 Bs.
Propósito:	● Rediseñar la red corporativa de datos en el Rectorado. ● Actualizar el equipamiento pasivo y activo de la red bajo normas. ● Mejorar los tiempos de respuestas en el acceso y funcionamiento de los servicios de información. ● Configurar el equipamiento nuevo y usado de la red para así facilitar la administración de toda la infraestructura de red. ● Crear el ambiente idóneo para la puesta en producción de nuevos servicios de información. ● Implantar medidas de seguridad enmarcadas en los estándares internacionales de seguridad como son los 7 niveles manejados por OSI, que va desde el aspecto físico hasta el control de las aplicaciones o servicios de información. ● Facilitar la administración de los recursos tecnológicos, ancho de banda y el servicio a los usuarios. ● Actualizar el direccionamiento lógico (IP) de los equipos activos que conforman la infraestructura de red del rectorado adaptándolos al nuevo diseño físico y lógico de la misma. ● Documentar de forma detallada toda la estructura tanto física como lógica de la red para prestar soporte a los usuarios de forma óptima.
Alcance:	Se instaló un nuevo equipamiento activo de hardware como son: Switches modulares capa 3 con velocidades de 10/100/1000 Mbps, Router modular para comunicación externa, Firewall para controlar y asegurar el acceso a los servicios y aprovechó una porción del equipamiento existente; se instaló cableado estructurado UTP categoría 6 para 200 puntos de datos y usó los que se encontraban instalados y certificados en las instalaciones del Nuevo Rectorado; se instaló y certificará un enlace de Fibra Óptica Multimodo y a su vez lo empalmó con un enlace que va hacia el V.R. Académico, esto se a llevó cabo a través de una empresa externa; se sacó provecho a un enlace funcional de fibra Óptica Multimodo que llega al Edif. Electrónica para interconectar a la Unidad Central de Planificación. También se configuró todo el equipamiento activo antes mencionado como son: creación y asignación de VLAN, enrutamiento de VLAN y segmentos de red a gran velocidad por medio de Switch Capa 3, filtrado de tráfico por (dirección MAC, IP, Protocolo, Puertos), calidad de servicio (QoS), control de tráfico hacia servidores y estaciones de trabajo, administración y control del ancho de banda entre otros. Se garantizó el funcionamiento y la operatividad de los Servicios de Información actuales y los que se implantarán a futuro; también se llevó a cabo la reubicación tanto física como lógica de los servidores para servicios privados y públicos en zonas controladas. Se documentó en forma detallada toda la infraestructura de red, se creó el libro de vida de la red y se realizó la ingeniería de detalle para administrar y controlar toda la infraestructura de la red tanto física como lógicamente.

Nota: Autor (2006).

Factibilidad Económica

La Universidad ha cubierto hasta los momentos la inversión en lo que respecta al área de tecnología y específicamente a lo concerniente a seguridad, a continuación se detallan en el cuadro 23:

Cuadro 23
Resumen de proyectos

Proyecto	Costo
Garantía Funcional Fase I (2.006-2007)	206.304.100,00
Normalización de Plataforma en las Estaciones de Trabajo (2.005-2006)	107.497.082,18
Rediseño y Actualización de la Infraestructura de Red del Rectorado (2.005-2006)	323.003.967,29
Total	636.805.149,47

Nota: Autor (2006).

Análisis costo/beneficio

Los costos deben estar asociados a cuanto vale la información, por ejemplo; el que sea cambiada la nómina del personal, una nota de estudiante, dar un título ha alguien que no ha estudiado en la Universidad, el no poder realizar los tramites académicos-administrativos por interrupción de los servicios, etc.

Como se evidencia en todas ellas la reputación de nuestra casa de estudios se encontraría en entredicho, por no decir menos, es allí donde la seguridad juega un papel preponderante en el tratamiento de la información.

Una vez analizado la factibilidad operativa, técnica y económica se corroboró que el diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica “Antonio José de Sucre” sede Rectoral es viable.

Fase III: Diseño del Plan de Seguridad Informática

En concordancia con la norma, se tomó como referencia el modelo de implantación PDCA (Plan-Do-Check-Act) contemplando la primera etapa, para desarrollar lo concerniente al diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral. En el (Anexo "B") se detalla el gantt y las actividades y sub-actividades son mostradas en el cuadro 24:

Cuadro 24
Diseño del Plan de Seguridad Informática

3.1. Establecimiento del SGSI (Plan)	
3.1.1. Inicio del Proyecto	● Asegurar el compromiso de la dirección. ● Seleccionar y entrenar a los miembros del equipo inicial que participan en el proyecto.
3.1.2. Definición del SGSI	● Identificación del alcance del SGSI y de la Política de Seguridad del SGSI. ● Recopilar los documentos de seguridad existentes en la organización.
3.1.3. Evaluación de Riesgos	● Definición de una metodología para la clasificación de los riesgos. ● Creación de un inventario de activos. ● Identificación y tasación de activos. ● Identificación de requerimientos de seguridad. ● Evaluación de la posibilidad de que las amenazas y vulnerabilidades ocurran. ● Cálculo de los riesgos de seguridad.
3.1.4. Tratamiento de Riesgos	● Selección de opciones de tratamiento de riesgos apropiadas. ● Selección de controles para reducir el riesgo a nivel aceptable.

Nota: Autor (2006).

3.1. Establecimiento del SGSI (Plan)

3.1.1. Inicio del Proyecto: Se inició con la adquisición y lectura del estándar internacional ISO/IEC 27001. Para clarificar el alcance del estándar se adoptó por asistir a cursos de formación impartidos por organismos certificadores.

- Asegurar el compromiso de la dirección: Este aspecto está presente, hecho confirmado por resolución del Consejo Universitario donde se establece el Reglamento de Tecnología y Servicios de Información (ver "http://www.unexpo.edu.ve/documentos/05-E09-05.pdf").
- Seleccionar y entrenar a los miembros del equipo inicial que participan en el proyecto: El Coordinador Nacional de Tecnología de Información recibió adiestramiento en "Auditoría en Sistemas de Gestión de Seguridad de la Información" dictado por Fondonorma; "Fundamentos de Seguridad en Redes de Datos" dictado por la Universidad Centrooccidental Lisandro Alvarado (UCLA). Esto con el fin de servir de multiplicador de los adiestramientos recibidos al personal asignado al área de seguridad dentro de la institución.

3.1.2. Definición del SGSI: Durante esta fase se definió el alcance del SGSI y se registró en un documento en el que se decidió que el sistema va hacer aplicado en la UNEXPO sede rectoral.

- Identificación del alcance del SGSI y de la Política de Seguridad del SGSI: Por razones de seguridad, la información que se refleja a continuación es de carácter confidencial, solo se tomó como referencia por motivos académicos el análisis de un servicio de información, siendo este, el alcance para la ejecución en el cual se han cambiado algunos ítems y ocultados otros que se consideraron críticos, sin menosprecio de la calidad brindada para la ejecución de la presente investigación y como ejemplo de lo implementado. 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 y así poder generar información oportuna, actualizada y consolidada, para cada uno de los niveles de la Organización, además de ser moldeable a los nuevos cambios en cuánto a leyes y de fácil adecuación a las nuevas tecnologías. El método utilizado para determinar el alcance fue el de las elipses; ver gráfico 15.

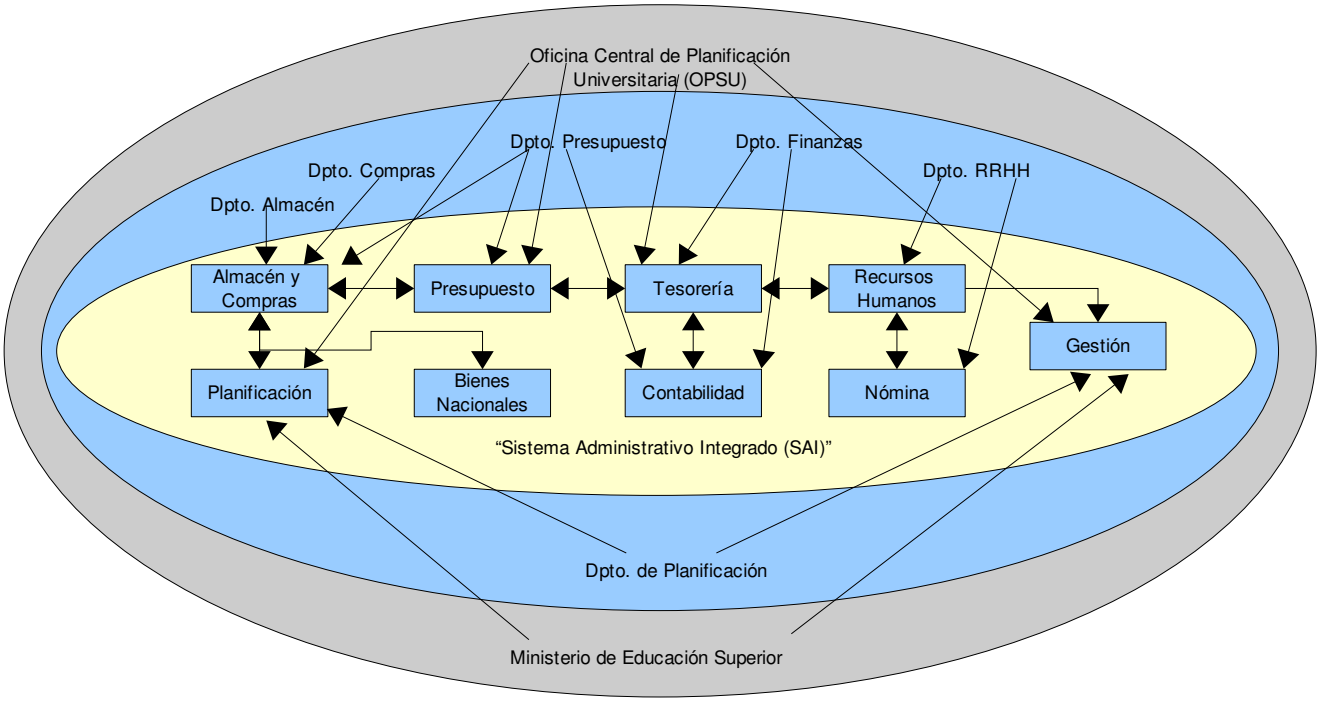


Gráfico 15. Metodología de las elipses. Caso Sistema Administrativo Integrado SAI
Nota: Autor (2006).

Sanz (2.006) explica que: "el plan de seguridad consiste en una serie de normas, procedimientos y políticas que se implantan en la estructura de una organización". En este sentido, seguidamente se muestra lo indicado por Sanz, es importante resaltar que lo descrito a continuación está bajo formato especial (forma):

Según lo indicado se muestra a continuación el primer elemento del Plan de Seguridad: las políticas de seguridad.

POLITICAS DE SEGURIDAD

I. Exposición de motivos

En la Universidad Experimental Politécnica "Antonio José de Sucre" UNEXPO, han ocurrido incidentes de seguridad en los servicios de información, ataques de denegación de servicio al servidor DNS (Domain Name System), presencia de correo SPAM (correo electrónico basura) de manera cotidiana, perdida o eliminación involuntaria de información institucional en los computadores de usuarios administrativos, computadores infectados de virus, troyanos y la no existencia de un plan de seguridad de la información que logre minimizar los riesgos ante las amenazas.

Ante la problemática planteada se presenta esta propuesta de políticas de seguridad que en materia de informática y de comunicaciones digitales debe poseer la Universidad para normar estos rubros.

II. Objetivos

Objetivo General

Establecer el marco de referencia para la administración de los recursos tecnológicos de la UNEXPO, tomando como referencia estándares internacionales.

Objetivo Específicos

- Establecer los alcances de las normas de seguridad informática.
- Definir las normas de seguridad informáticas.
- Definir las sanciones de acuerdo al no cumplimiento de las normas de seguridad.

III. Bases legales

Estándares Internacionales

- ISO/IEC 27001:2005 Sistemas de gestión de seguridad de la información – Requerimientos. Organización Internacional de Estándares (ISO).
- ISO/IEC 17799:2005 Código para la práctica de la gestión de la seguridad de la información Organización Internacional de Estándares (ISO).
- Lineamientos OECD para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad.

Leyes Nacionales

- 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.

- Ley Sobre Mensajes de Datos y Firmas Electrónicas 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.
- Ley Orgánica de Telecomunicaciones, promulgada 12 de junio de 2000 y publicada en Gaceta Oficial No.36.970. Caracas - Venezuela.

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

IV. Concepto política.

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

Principios que pretende brindar la presente política de seguridad:

- **Integridad:** requiere que la información solo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de mensajes trasmitidos.
- **Confidencialidad:** requiere que la información sea accesible únicamente por las entidades autorizadas.
- **Disponibilidad:** requiere que los elementos del sistema informático estén disponibles para las entidades autorizadas cuando los necesiten.
- **No repudio:** ofrece protección a un usuario frente a otro usuario que nieguen posteriormente que se realizo cierta comunicación. esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. el no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje.

V. Políticas de seguridad

La Oficina Central de Tecnología y Servicios de Información (OCTSI) está conformada por tres Coordinaciones Nacionales, y una Dirección. Las coordinaciones son de Atención a Usuarios, Producción y Operaciones, Tecnología de Información, estás son las encargadas de brindar servicio al usuario, por el ámbito de competencia que tiene cada una de ellas en materia de informática. Así pues este apartado contiene una clasificación de estas políticas, y son:

Del equipo

De la instalación de equipo de cómputo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, supercomputadoras, y equipo accesorio), que esté o sea conectado a la Red de la UNEXPO, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse a las normas y procedimientos de instalación que emite la OCTSI.
2. El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en una área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica, su acceso que la OCTSI tiene establecido en su normativa de este tipo.
3. Los responsables de las áreas de apoyo administrativo de las direcciones y departamentos deberán en conjunción con la OCTSI dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.
4. La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a las autoridades correspondientes (departamento de Bienes Nacionales, OCTSI y otros de competencia).

Del mantenimiento de equipo de cómputo.

1. A la OCTSI corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.
2. En el caso de los equipos atendidos por terceros la OCTSI deberá normar al respecto.
3. El personal técnico de apoyo interno de los departamentos académicos se apegará a los requerimientos establecidos en las normas y procedimientos que la OCTSI emita.
4. Los responsables de las áreas de Cómputo de un departamento pueden otorgar mantenimiento preventivo y correctivo, a partir del momento en que sean autorizados por la OCTSI.
5. Corresponde a la OCTSI dar a conocer las listas de las personas, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.

De la actualización del equipo.

1. Todo el equipo de cómputo (computadoras personales, estaciones de trabajo, supercomputadora y demás relacionados), y los de telecomunicaciones que sean propiedad de la UNEXPO debe procurarse sea actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

De la reubicación del equipo de cómputo.

1. La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que Bienes Nacionales y la OCTSI emitan para ello.
2. En caso de existir personal técnico de apoyo de los departamentos académicos, éste notificará de los cambios tanto físicos como de software de red que realice a la OCTSI, y en su caso si cambiará de responsable (el equipo) a Bienes Nacionales y OCTSI.
3. El equipo de cómputo a reubicar de la UNEXPO se hará únicamente bajo la autorización del responsable, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

Del control de accesos

Del acceso a áreas críticas.

1. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta la OCTSI.
2. La OCTSI deberá proveer de la infraestructura de seguridad informática requerida con base en los requerimientos específicos de cada área.
3. Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

Del control de acceso al equipo de cómputo.

1. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que la OCTSI emita.
3. Las áreas de cómputo de los departamentos donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítica, deberán sujetarse también a las normas que establezca la OCTSI.
4. Los accesos a las áreas de críticas deberán de ser clasificados de acuerdo a las normas que dicte la OCTSI de común acuerdo con su comité de seguridad informática.
5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la OCTSI tiene la facultad de acceder a cualquier equipo de cómputo que no estén bajo su supervisión.

Del control de acceso local a la red.

1. La OCTSI es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
2. La OCTSI es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.
3. Dado el carácter unipersonal del acceso a la Red UNEXPO, la OCTSI verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.
4. El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, equipo de supercómputo centralizado y distribuido, etc.) conectado a la red es administrado por la OCTSI.
5. Todo el equipo de cómputo que esté o sea conectado a la Red UNEXPO, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite la OCTSI.

De control de acceso remoto.

1. La OCTSI es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
2. Para el caso especial de los recursos de supercómputo a terceros deberán ser autorizados por la Dirección o por las autoridades nacionales.
3. El usuario de estos servicios deberá sujetarse al Reglamento de uso de la Red UNEXPO y en concordancia con los lineamientos generales de uso de Internet.
4. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la OCTSI.

De acceso a los sistemas administrativos.

1. Tendrá acceso a los sistemas administrativos solo el personal del UNEXPO que es titular de una cuenta de gastos o bien tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.
2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.
3. La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la Red UNEXPO y por las normas y procedimientos establecidos por la OCTSI.
4. Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal de la OCTSI.

5. El control de acceso a cada sistema de información de Administrativa será determinado por la unidad responsable de generar y procesar los datos involucrados.

Del Word Wide Web.

1. La OCTSI es el responsable de instalar y administrar el o los servidor(es) WWW. Es decir, sólo se permiten servidores de páginas autorizados por la OCTSI.
2. La OCTSI deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.
3. Los accesos a las páginas de web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la Red UNEXPO.
4. A los responsables de los servidores de Web corresponde la verificación de respaldo y protección adecuada.
5. Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos que la OCTSI emita.
6. El material que aparezca en la página de Internet de la UNEXPO deberá ser aprobada por la OCTSI, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).
7. Con referencia a la seguridad y protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por la OCTSI.
8. La OCTSI tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

<u>De utilización de los recursos de la red</u>

1. Los recursos disponibles a través de la Red UNEXPO serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de la Universidad.
2. La OCTSI es la responsable de emitir y dar seguimiento al Reglamento para el uso de la Red.
3. Corresponde a la OCTSI administrar, mantener y actualizar la infraestructura de la Red UNEXPO.
4. Dado el carácter confidencial que involucra el correo electrónico la OCTSI emite su reglamentación.

Del Software

De la adquisición de software.

1. La OCTSI es el ente oficial de la Universidad para establecer los mecanismos de procuración de sistemas informáticos.
2. La OCTSI propiciará la adquisición de licencias de sitio, licencias flotantes, licencias por empleado y de licencias en cantidad, para obtener economías de escala y de acorde al decreto 3390 de la república Bolivariana de Venezuela.
3. Corresponderá a la OCTSI emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia en concordancia del decreto 3390 de la república Bolivariana de Venezuela.
4. De acuerdo a los objetivos globales de la OCTSI se deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.
5. En cuanto a la los software sin costo deberá respetarse la propiedad intelectual intrínseca del autor.
6. La OCTSI promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
7. La OCTSI deberá promover el uso de sistemas programáticos que redunden en la independencia de la institución con los proveedores.

De la instalación de software.

1. Corresponde a la OCTSI emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.
2. En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.
3. La OCTSI es la responsable de brindar asesoría y supervisión para la instalación de software informático y para el software de telecomunicaciones.
4. La instalación de software que desde el punto de vista de la OCTSI pudiera poner en riesgo los recursos de la institución no está permitida.
5. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).
6. La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento a la OCTSI.

De la actualización del software.

1. La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a la calendarización que anualmente sea propuesta por la OCTSI.
2. Corresponde a la OCTSI autorizar cualquier adquisición y actualización del software.
3. Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por la OCTSI.

De la auditoría de software instalado.

1. El departamento de Auditoría Interna de la UNEXPO es la responsable de realizar revisiones periódicas para asegurar que sólo programación con licencia esté instalada en las computadoras de la institución.
2. La OCTSI propiciará la conformación de un grupo especializado en auditoría de sistemas de cómputo y sistemas de información.
3. Corresponderá al grupo especializado dictar las normas, procedimientos y calendarios.

Del software propiedad de la institución.

1. Toda la programática adquirida por la institución sea por compra, donación o cesión de auditoría es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera.
2. La OCTSI deberá tener un registro de todos los paquetes de programación propiedad de la UNEXPO.
3. Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfases) desarrollados con o a través de los recursos de la UNEXPO se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.
4. Es obligación de la OCTSI, mantener los respaldos correspondiente de la información institucional ya que se considera como un activo de la Universidad que debe preservarse.
5. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.
6. Corresponderá a la OCTSI promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos.
7. La OCTSI propiciará la gestión de patentes y derechos de creación de software propiedad de la institución.
8. La OCTSI administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

Sobre el uso de software académico.

1. Cualquier software que requiera ser instalado para trabajar sobre la Red UNEXPO deberá ser evaluado por la OCTSI.
2. Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la Universidad.

De supervisión y evaluación

1. Cada uno de las coordinaciones de la OCTSI donde esté en riesgo la seguridad en la operación, servicio y funcionalidad del departamento, deberá emitir las normas y los procedimientos que correspondan.
2. Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca la OCTSI y/o el grupo especializado de seguridad.
3. Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet disponen.
4. Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

Generales.

1. Cada uno de los departamentos deberán de emitir los planes de contingencia que correspondan a las actividades críticas que realicen.
2. Debido al carácter confidencial de la información, la OCTSI deberá de conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

Sanciones.

1. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la OCTSI.
2. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.
3. Corresponderá a la OCTSI hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.
4. Todas las acciones en las que se comprometa la seguridad de la Red UNEXPO y que no estén previstas en esta política, deberán ser revisadas por la OCTSI para dictar una resolución sujetándose al estado de derecho.

Notas

1. Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.
2. El documento que contiene la política de seguridad deber ser difundido a todo el personal involucrado en la definición de estas políticas.

El segundo elemento del Plan de Seguridad: Procedimientos.

PROCEDIMIENTOS DE SEGURIDAD EN RESPALDO

1. CUADRO DE CONTROL

Versión	Fecha	Descripción
1.0	04/10/2005	"Aspectos Técnicos a Contemplar Para Realizar procesos de almacenamiento y respaldo"

2. LUGAR

LA UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA "ANTONIO JOSE DE SUCRE" , SEDE RECTORAL.

3. INTRODUCCION

La Oficina Central de Tecnología y Servicios de Información (OCTSI) en uso de las atribuciones legales que le confiere el artículo 7 del REGLAMENTO DE TECNOLOGIA Y SERVICIOS DE INFORMACION DE LA UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA "ANTONIO JOSE DE SUCRE" aprobado en sesión extraordinaria de Consejo Universitario No 2005-E09 de Fecha 04 de mayo de 2005 y según resolución No 2004-E14 de fecha 20 de Julio de 2004 establece las bases técnicas a seguir a la hora de llevar a cabo procesos de Almacenamiento y Respaldo dentro de las instalaciones de la UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA "ANTONIO JOSE DE SUCRE". Definición, desarrollo o implementación de estrategias para el respaldo de la información de los servicios asociados con los servidores institucionales.

Cuando se habla de Políticas se hace referencia a un conjunto de normas o reglas que rigen, desde lo más general hasta lo más detallado, cualquier actividad operativa.

Las políticas de respaldo describen, específicamente, el esquema a seguir cuando se crean o modifican nuevos procesos de resguardo de datos, indicando que tipo de datos respaldar, de que forma respaldarla, cuando se debe respaldar; así como describir en que forma se deben crear nuevos objetos dentro de la herramienta de respaldo, sean nombres de configuraciones de respaldo, nombre de dispositivos de respaldo, nombres de grupos de cintas y etiquetas de las cintas.

Este tipo de actividades permiten a los operadores de un centro de cómputo o de datos:

- Visualizar los objetos de forma estandarizada,
- Obtener rápidamente información de los objetos que se están manejando sin necesitan de profundizar más en la configuración,

- Transferir el conocimiento de la operación de los procesos de respaldo, de un operador a otro, sin mayor dificultad, y
- Hacer de la actividad de operaciones algo menos empírico.
- Este documento servirá como una guía, la cual debe ser constantemente retroalimentada con cualquier nueva política que se logre definir de la operación diaria y, que permita que la administración de los procesos de respaldo sea cada vez más versátil. Garantizando la integridad y disponibilidad de la información en caso de eventuales desastres, errores de borrado de la información y/o en fallas del hardware y software; minimizando el impacto producido por la pérdida o corrupción de datos.

Hay que mantener como premisa que los datos resguardados no tienen importancia hasta que se requiere restaurarlos. En este sentido, toda política de respaldo debe ser diseñada pensando en cuan práctico, fácil y rápido será el procedimiento de restauración de los datos.

4. Definiciones y abreviaciones

4.1. Tipos de Datos

Los datos existentes en un servidor cualquiera se pueden clasificar de la siguiente manera:

4.1.1. Archivos

Considera cualquier archivo que puede estar almacenado en un servidor, excluyendo los correspondientes a una base de datos. Los podemos subdividir en:

- **SISTEMA OPERATIVO**: Archivos binarios, ejecutables y configuración del Sistema de Operación.
- **APLICACIONES**: Archivos binarios, ejecutables y de configuración de la(s) aplicación(es) instaladas en un servidor.
- **DATOS:** Archivos de información generados por los usuarios y aplicaciones, y almacenados en el servidor.

4.1.2. Base de datos

Los archivos de base de datos se pueden respaldar de diferentes formas dependiendo del manejador debase de datos que se emplee:

- **ONLINE:** Esta forma permite respaldar una base de datos ”en caliente” o “en línea” y la ejecución del respaldo se hace mientras la base de datos está en uso.
- **OFFLINE**: Esta forma de respaldar una base de datos requiere la configuración y empleo de unos scripts que permitan detener e iniciar el funcionamiento de la base de datos. Los objetos a respaldar son los mismos que en formato ONLINE, pero en formato FILESYSTEM, más ciertos archivos necesarios para

poder llevar a cabo la recuperación completa. Durante la ejecución del respaldo la base de datos debe estar detenida.

- **LOGS / ARCHIVES**: Son todos aquellos archivos que reflejan las transacciones realizadas (committed) y no realizadas sobre la base de datos, durante su ejecución.

Tipos de Respaldo

Existen dos tipos básicos de respaldos del tipo FILESYSTEM: full e incremental. Un respaldo FULL guarda todos los archivos seleccionados para un respaldo. Un respaldo INCREMENTAL guarda solo aquellos archivos que han cambiado desde el último respaldo FULL o INCREMENTAL.

Respaldo	Archivos en respaldo	Archive bit	Ventajas	Desventajas
Completo ("Full")	Siempre resguarda todos los objetos seleccionados aún cuando no haya cambiado desde el respaldo previo	Eliminado en todos los archivos	Con este respaldo únicamente es posible recuperar toda la información Permiten restauraciones más rápidas y simples. Para obtener la última versión de los archivos, se requiere solamente la media (cartucho) del último respaldo FULL Permiten restauraciones más rápidas y simples. Para obtener la última versión de los archivos, se requiere solamente la media (cartucho) del último respaldo FULL. Proveen una mayor confiabilidad. Todos los datos son respaldados en una sesión de respaldo y su restauración es relativamente simple	Toman más tiempo en realizarse. Se tiene varias veces la misma versión de los archivos respaldados, ocupando más espacio en la media y en la base de datos de la herramienta de respaldo.

Respaldo	Archivos en respaldo	Archive bit	Ventajas	Desventajas
De Incremento ("Incremental")	Archivos con archive bit activo. Resguarda los cambios realizados desde el último respaldo FULL o INCREMENTAL.	Eliminado en los archivos que se respaldan	Ocupan menos espacio en la media (cartucho). Ocupan menos espacio en la base de datos de la herramienta de respaldo. Toman menos tiempo para realizarse, ya que, respaldan una cantidad de datos menor.	La restauración toma mayor tiempo, ya que, los datos deben ser restaurados desde el último FULL y todos los INCREMENTAL realizados subsecuentemente hasta la fecha deseada. La restauración requiere de más media, ya que, el FULL y los INCREMENTAL pueden no estar en el mismo medio.
Diferencial ("Differential")	Archivos con archive bit activo.(Aquellos que hayan cambiado desde el último Respaldo Completo)	Intacto	Sólo requiere del último Respaldo Completo y del último respaldo Diferencial	Ocupa mayor espacio en discos comparado con Respaldos de Incremento

Tipos de respaldos INCREMENTAL

La herramienta de respaldo debe proveer respaldos incrementales de diferentes tipos:

INC	: Este tipo de respaldo, toma como referencia el último respaldo realizado cualquiera sea su tipo, sea un respaldo FULL o un respaldo INCREMENTAL (sea INC o INC#), el cual debe estar aún protegido, es decir, su retención no ha expirado aún. Este respaldo también es llamado *respaldo diferencial*, ya que, solamente toma los cambios realizados desde el respaldo previo.
INC 1-9	: Un respaldo INCREMENTAL por nivel, tomo como referencia el último respaldo del nivel inferior más cercano, que aún esté protegido. Por ejemplo, un respaldo INC1 respalda los cambios desde el último respaldo FULL, mientras que un respaldo INC5 respalda los cambios desde el último INC4. Un respaldo INC# nunca toma como referencia un respaldo INC previo.

4.3. Retención o Protección de Datos

La herramienta de respaldo debe permitir especificar cuanto tiempo se debe mantener los datos respaldados en la media (cartucho), y cuanto tiempo se debe mantener la información de los datos respaldados, en la base de datos de la herramienta.

4.4. Rotación de medios (cartuchos)

Procedimiento operativo que indica la movilización de cartuchos de cintas dentro de un dispositivo de respaldo cuando se presenten situaciones tales como:

- El grupo (pool) de cartuchos asociado a un proceso de respaldo se llenó de datos y requiere la inclusión de cartuchos nuevos.
- Los procedimientos de respaldo exigen la salida de ciertos cartuchos después de realizarse algún tipo de respaldo especial, por ejemplo, Full Mensuales o Anuales.

Este procedimiento responde a una serie de cálculos que el operador debe realizar para poder obtener el índice de rotación.

Antes de ejecutar el cálculo, el operador debe establecer o fijar dos constantes:

1. un período de referencia (una semana, quince días, un mes, etc.) que quiere usar para determinar la cantidad de datos que se respalda y con que rapidez se llena el pool en ese período. Este período debería incluir uno o más ciclos o generaciones completas de respaldo de un tipo de datos en particular. Por ejemplo:

Si se tiene un esquema de respaldo donde se realizan un (1) respaldo FULL semanal y seis (6) respaldos INCREMENTAL por día, del mismo tipo de datos, los períodos de referencia a evaluar deberían ser múltiplos de siete (7) días, debido a que el ciclo completo dura siete días. Entonces se podría acotar el cálculo a períodos de referencia de: siete (7) días, catorce (14) días, veintiún (21) días o cualquier valor múltiplo de 7.

2. la cantidad de ranuras (slots) que se le asignará a un pool de cintas.

Una vez fijadas estas constantes, el índice de rotación se calcularía de la siguiente forma:

Donde,

$$IR = \mathrm{Re}\,dondeoAbajo\left(\frac{\mathrm{Re}\,dondeoArriba\left(\frac{\left|¿FULL * CapFULL + ¿INC * CapINC\right| * \#Ciclos}{CapMEDIA}\right)}{¿Slots}\right)$$

IR: es un valor numérico que indica cuantas veces se tendrán que rotar los medios contenidos en un pool.

#FULL: indica la frecuencia de ejecución de un respaldo FULL dentro de un ciclo o generación completa. Generalmente, este valor es uno (1). En el ejemplo, el valor de esta variable es uno (1).

#INC: indica la frecuencia de ejecución de un respaldo INCREMENTAL dentro de un ciclo o generación completa. En el ejemplo, el valor de esta variable es seis (6).

CapFULL: cantidad de datos, expresada en GB, que se respalda en un respaldo FULL. Esta información puede ser de tipo estadística y puede ser obtenida de las sesiones de respaldo ya realizadas.

CapINC: cantidad de datos, expresada en GB, que se respalda en un respaldo INCREMENTAL. Esta información puede ser de tipo estadística y puede ser obtenida de las sesiones de respaldo ya realizadas. Puede usarse como valor aproximado, el 10% de la cantidad de datos respaldada en un FULL.

#Ciclos: cantidad de veces que se repite un ciclo o generación completa de respaldo, dentro del período de referencia.

5. Políticas

5.1. Bases de datos

En este punto el alcance abarca cualquier base de datos, sea Oracle, Access, MS-SQL, y cualquier otra soportada por la herramienta de respaldo, las cuales pueden ser divididas en sus diferentes ambientes de uso:

- Producción,
- Desarrollo,
- Quality Assurance (QA),
- Data WareHouse (DWH).

Las políticas de respaldo de bases de datos para el ambiente de PRODUCCIÓN y DATA WAREHOUSE son las siguientes:

- Los respaldos de bases de datos deben realizarse en forma ONLINE. Los respaldos ONLINE deben realizarse diariamente, como mínimo una (1) vez al día. Preferiblemente en horas de poca carga en el servidor.
- Cada respaldo debe ser de manera FULL, debe incluir toda la estructura de la base de datos y sus datos.
- Los respaldos de estos archivos debe realizarse como mínimo dos (3) veces al día borrando los archivos una vez respaldados, ya sea, cada vez que se ejecute el respaldo, o cuando se ejecute algún respaldo específico en el día.
- Se realizaran respaldo semanal OFFLINE, además de incluir el directorio de BD, debe incluir el directorio donde se encuentran almacenados los archivos de transacciones y todos aquellos archivos que ofrezcan integridad a la BD, como los archivos de control, índices, en aquellos manejadores de BD donde aplique. La retención de estos respaldos será de cuatro (4) semanas.
- Los respaldos diarios o semanales se destinarán a un (1) pool de cintas diferente para cada BD.
- La retención o vigencia de estos respaldos semanales será de cuatro (4) semanas.
- Se realizarán respaldos nivel cero mensuales de tipo OFFLINE, lo cual incluye toda la estructura y data del servidor (incluye la configuración del sistema operativo y la base de datos offline). Los mismos tendrán una retención de tres (3) meses. La rotación de los cartuchos o cintas se realizará semanalmente.
- Para la ejecución de los respaldo OFFLINE, los filesystems de BD podrán ser respaldados empleando scripts especiales para detener el manejador durante el respaldo y luego iniciarlo, al terminar el respaldo.

Componente	Periodicidad			Retención		Rotación
	Diaria	Semanal	Mensual	Semanas	Mensual	
Base de Datos OFFLINE		**X**		**4**		
Base de Datos ONLINE	X					
Archive Log (3) veces o file system > 70%	X					
Aplicativo	X					
Base de Datos OFFLINE - Full Equipo			**X**		**3**	

Las políticas de respaldo de bases de datos para el ambiente de DESARROLLO y QUALITY ASSURANCE son las siguientes:

- Los respaldos Offline deben realizarse mensualmente. Preferiblemente en horas de poca carga en el servidor.
- Cada respaldo debe ser de manera FULL, debe incluir toda la estructura de la base de datos y sus datos.
- La retención o vigencia de estos respaldos debe ser establecida por los usuarios y responsables de estas bases de datos, pero debe ser mínimo de 4 semanas.

5.2. Políticas para los Archivos Convencionales

El alcance de este punto abarca todos los archivos de cada servidor: los archivos del Sistema Operativo, archivos que constituyen las aplicaciones, archivos que generan las aplicaciones, los archivos creados por los usuarios y los archivos de las BD cuando el manejador se encuentra fuera de línea.

Las políticas de respaldo de estos archivos y sus respectivos servidores, son las siguientes:

5.2.1. ARCHIVOS DE SISTEMA OPERATIVO

- Este tipo de archivos, siempre debe ser respaldado para efectos de Recovery, y por ende deben ser manejados en los procesos de Disaster Recovery.

- Se realizarán respaldos discrecionales de tipo FULL de los filesystems necesarios, cuando ocurran cambios del tipo: instalación de parches, nuevas versiones de un módulo, o cualquier evento que ocasione un cambio en los archivos que conforman el sistema operativo. Se recomienda un respaldo mensual como mínimo. En caso de actualizaciones por cambio de hardware, cambio de aplicación, cambio de base de datos, instalación de patches o cambios de versión; los respaldos se harán antes y después de la(s) actualización(es).
- Los respaldos mensuales se destinarán a un (1) pool de cintas, preferiblemente diferente para cada servidor.
- La retención o vigencia de estos respaldos mensuales puede ser de tres (3) meses.
- La rotación de los cartuchos o cintas se realizará mensualmente.
- Para los sistemas operativos, deben implementarse respaldos, teniendo en cuenta los siguientes acuerdos:
    - Respaldando los directorios donde se encuentra la configuración del sistema operativo
    - Creando los diskettes de arranque en caso de que el sistema operativo lo permita
    - Semanalmente para todos los servidores con Windows y Linux
    - Los respaldos se harán por servidor.

5.2.2. ARCHIVOS DE APLICACIONES

- Se realizarán respaldos discrecionales de tipo FULL de los filesystems necesarios, cuando ocurran cambios del tipo: instalación de parches, nuevas versiones de un módulo, o cualquier evento que ocasione un cambio en los archivos que conforman la aplicación. Se recomienda un respaldo mensual como mínimo. Preferiblemente en horas de no acceso de los usuarios al servidor.
- Los respaldos mensuales se destinarán a un (1) pool de cintas, preferiblemente diferente para cada servidor.
- La retención o vigencia de estos respaldos mensuales puede ser de tres (3) meses.
- La rotación de los cartuchos o cintas se realizará mensualmente.

5.2.3. ARCHIVOS DE DATOS

Este tipo de archivos puede respaldarse en tres niveles: diarios, semanales y mensuales. Para los respaldos diarios, las políticas serán las siguientes:

- Se realizarán respaldos diarios tipo INCREMENTAL sobre los servidores que manejen archivos de datos, como mínimo una (1) vez al día. Preferiblemente en horas de no acceso de los usuarios al servidor.
- Los respaldos diarios se destinarán a un (1) pool de cintas diferente por cada servidor. La retención o vigencia de estos respaldos diarios puede ser mínimo de siete (7) días.
- La rotación de los cartuchos o cintas se realizará semanalmente.

Para los respaldos semanales, las políticas serán las siguientes:

- Se realizarán respaldos semanales de tipo FULL sobre los servidores que manejen archivos de datos, como mínimo una (1) vez a la semana. Preferiblemente en horas de no acceso de los usuarios al servidor.
- Los respaldos semanales se destinarán a un (1) pool de cintas diferente por cada servidor.
- La retención o vigencia de estos respaldos diarios puede ser mínimo de siete (7) días.
- La rotación de los cartuchos o cintas se realizará semanalmente.

Para los respaldos mensuales, las políticas serán las siguientes:

- Se realizarán respaldos mensuales de tipo FULL sobre los servidores que manejen archivos de datos, como mínimo una (1) vez al mes. Preferiblemente en horas de no acceso de los usuarios al servidor.
- Los respaldos mensuales se destinarán a un (1) pool de cintas diferente por cada servidor.
- La retención o vigencia de estos respaldos mensuales puede ser mínimo de tres (3) meses. La rotación de los cartuchos o cintas se realizará mensualmente.

El tercer elemento del Plan de Seguridad: las normas y procedimientos.

MANUAL DE NORMAS Y PROCEDIMIENTOS

No. DE VERSIÓN	FECHA DE VIGENCIA	RESPONSABLE ACTUALIZACIÓN	PRINCIPALES CAMBIOS REALIZADOS
1ra.	Julio 2005	CNPO	Primera versión del Manual de Normas y Procedimientos de la CNPO
2da.	Octubre 2005	CNPO	Segunda versión del Manual de Normas y Procedimientos de la CNPO

PARTICIPANTES EN LA ELABORACIÓN DEL MANUAL

UNIDAD
Coordinación Nacional de Producción y Operaciones (CNPO).
CNPO / Soporte de Servicio de Información
CNPO / Soporte de Ambiente Operativo.
CNPO / Soporte de Servicio de Información

INTRODUCCIÓN.

La Coordinación Nacional de Producción y Operación (CNPO) de la Oficina Central de Tecnología y Servicios de Información (OCTSI), adscrita al Rectorado de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" (UNEXPO), consciente de la carencia de manuales de instructivos normativos que regulen la actividad de los procesos de sus unidades, ha elaborado el presente Manual de Normas y Procedimientos, el cual permitirá al personal y a toda la institución consultar los procedimientos que involucran los procesos que conforman el funcionamiento de la coordinación. El mismo servirá como un instructivo administrativo que apoye al adiestramiento de un nuevo empleado el cual se realizará en menor tiempo y menor costo, también tiene la ventaja de comunicar oportunamente todos los cambios en las rutinas de trabajo que generen con el progreso de la coordinación.

En este manual se presentan los procedimientos correspondiente a la Coordinación Nacional de Producción y Operaciones, describiendo los pasos necesarios para llevar a cabo un procedimiento, así como los responsables de ejecutarlos, de una manera clara y ajustada a las bases legales y normativas de la Universidad, se presentan también los formularios e instructivos involucrados en los procedimientos.

Cabe destacar, que las acciones a seguir contenidas en el presente manual podrán optimizarse en la medida que los procesos sean cada vez prácticos, lo cual permite la flexibilidad adecuada en la búsqueda permanente de mayor eficiencia y efectividad en

el desempeño de las tareas a desarrollar, para alcanzar los objetivos y metas de la CNPO, así como también del mejoramiento continuo de sus procesos

PRESENTACIÓN

El Manual de Normas y Procedimientos de la Coordinación Nacional de Producción y Operaciones (CNPO) de la Oficina Central de Tecnología y Servicios de Información de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" (Unexpo) Rectorado, es el instrumento a través del cual esta coordinación documenta y comunica a toda la institución los lineamientos, normativas y procedimientos de la CNPO.

OBJETIVO DEL MANUAL

El Manual tiene como objetivo fundamental establecer las Normas y Procedimientos que realiza la CNPO, con el fin de servir como un elemento de información, decisión, y control en el nivel de desempeño y apoyo a la Unexpo, mediante el uso eficiente de la tecnología de la información en sus diferentes procesos operativos y administrativos.

INSTRUCCIONES Y USO DEL MANUAL

El presente manual de normas y procedimientos, ha sido elaborado con la finalidad de redefinir y normar todos los procedimientos que operan, en la Coordinación Nacional de Producción y Operaciones (CNPO), para documentar y optimizar su funcionamiento y desempeñar con eficiencia y calidad las diferentes actividades que enmarcan sus objetivos.

Para la correcta comprensión de este manual, se debe tomar en cuenta las siguientes indicaciones:

1.La aplicación efectiva y el desarrollo de los procedimientos operativos y administrativos aquí plasmados, recaen sobre el Coordinador de la unidad.

2.Cualquier cambio en el ordenamiento legal vigente, o en las políticas de la CNPO, que en materia de procedimientos afecten la estructura de esta coordinación, generará también un cambio en el contenido del presente manual con el fin de adaptarlo a las nuevas políticas aprobadas.

3.El contenido del presente manual sólo podrá ser modificado por el Comité Técnico de Control de Cambios (CTCC), cumpliendo con las instrucciones de la OCTSI.

4.Cualquier cambio necesario, será incorporado en este manual en el menor tiempo posible, con el fin de mantenerlo actualizado.

5.Los usuarios del manual, deberán notificar por escrito a la CNPO-OCTSI las sugerencias, modificaciones o cambios que afecten el contenido del mismo, con el

objeto de garantizar la vigencia de su contenido y con ello mejorar la base de conocimiento en el tiempo.

LINEAMIENTOS

1. Mantener la operatividad y funcionalidad de toda la infraestructura tecnológica y de servicios de información que dan soportes a la gestión académico-administrativo de la institución.
2. La CNPO estará dirigida por un coordinador, el cuál será designado por el Rector mediante postulación del Director de la OCTSI.
3. La CNPO está conformada por los siguientes grupos de trabajo: Soporte Ambiente Operativo, Soporte Servicios de Información y Soporte de Mantenimiento de Seguridad.
4. Garantizar el funcionamiento de la infraestructura de comunicaciones y el acceso a los servicios de información.
5. Administrar y Operar los servidores y plataforma de comunicaciones de uso por los diferentes servicios de información.
6. Establecer mecanismos de muestreo sobre la funcionalidad y diversidad de plataforma tecnológica en uso.
7. Realizar en forma permanente el inventario y control de los medios magnéticos de almacenamiento de la información.
8. Realizar en forma permanente el inventario de toda la infraestructura de Hardware y Software existente en la Institución, que sirve de soporte a los servicios de información, monitoreo de la utilización, crecimiento y actualización del software operativo.
9. Elaborar y ejecutar los planes de mantenimiento preventivo y correctivo de la infraestructura de hardware y software en producción.
10. Mantener y controlar un inventario básico de insumos y repuestos, que permitan garantizar la continuidad de funcionamiento de los equipos y sistemas.
11. Evaluar en forma continua el funcionamiento de todos los sistemas y resolver los problemas operativos y funcionales.
12. Establecer mecanismos de muestreo sobre la funcionalidad de los servicios de información en uso.
13. Realizar, mantener y garantizar la integridad de la información a través de procedimientos de respaldos.
14. Elaborar y ejecutar los planes de mantenimiento de los servicios de información en producción.
15. Mantener y controlar un inventario básico de insumos de software, que permitan garantizar la continuidad de funcionamiento de los equipos y sistemas.
16. Administrar todo el proceso de producción de los servicios de información.

17. Evaluar la calidad de los servicios de información en producción y aplicar los correctivos necesarios.
18. Definir e implantar normas y procedimientos para la asignación de prioridades y recursos requeridos para la producción de los servicios de información.
19. Aplicar las medidas de seguridad establecidas para la operación y funcionamiento de los recursos tecnológicos y de información de la institución.
20. Realizar el monitoreo continuo de la seguridad, en la plataforma tecnológica de la institución.
21. Llevar estadísticas sobre intentos de acceso no autorizados a los servicios de información y la red corporativa de datos de la institución.
22. Garantizar la seguridad en el intercambio de información entre los usuarios y los servicios de información en producción.

NORMAS GENERALES

La Coordinación Nacional de Producción y Operaciones, canalizará todas aquellas solicitudes de servicios que ingresen a ella, y las mismas serán analizadas y discutidas por la Coordinación y unidades a su cargo.

NORMA
CREACIÓN DE CUENTAS A USUARIOS

1. La CNPO tramitará sólo aquellos requerimientos recibidos por la Coordinación Nacional de Atención al Usuario (CNAU) recibidos a través del sistema Helpdesk.
2. La CNPO será la encargada de la creación y mantenimiento de las cuentas de dominio y de correo de la UNEXPO.
3. Las claves de acceso podrán ser modificadas por el usuario cuando lo desee o cuando sea necesario por medidas de seguridad.
4. Toda cuenta de correo deberá estar asociada a la cuenta de dominio del usuario.
5. Las configuraciones de las cuentas de correo serán realizadas localmente en la estación de trabajo del usuario por parte de la CNAU.
6. La CNPO realizará mantenimiento preventivo a los servidores de correo cada quince (15) días.

PROCEDIMIENTO
CREACIÓN DE CUENTAS A USUARIOS

RESPONSABLE	ACCIÓN
COORDINACIÓN NACIONAL DE PRODUCCIÓN Y OPERACIONES	1. **Recibe** de la CNAU, mediante el sistema Helpdesk, el requerimiento para efectuar la creación de cuenta al personal de la UNEXPO.
	2. **Asigna** a través del sistema Helpdesk el responsable de la asignación.
ANALISTA	3. **Consulta** en el sistema Helpdesk la asignación.
	4. **Verifica** los datos del usuario para la creación de la cuenta. o **En caso de no estar completos los datos requeridos**, documenta el ticket e informa a la CNPO.
	5. **Crea** la cuenta requerida de acuerdo con lo dispuesto en el instructivo de "Creación de cuentas de dominio y de correo a usuarios".
	6. **Verifica** que la creación de la cuenta sea satisfactoria. o **En caso de no ser satisfactoria**, procede de acuerdo a lo descrito en el punto 5 de este procedimiento.
	7. **Registra** la información en el sistema Helpdesk indicando el resultado e informa a la CNPO.
	8. **Consulta** en el sistema Helpdesk la respuesta de la asignación.
COORDINACIÓN NACIONAL DE PRODUCCIÓN Y OPERACIONES	9. **Envía** mediante el sistema Helpdesk el ticket a la CNAU para que realice el procedimiento de instalación de los servicios de red.

NORMA
ACTUALIZACIÓN DE INFRAESTRUCTURA DE RED

1. La CNPO será la encargada de efectuar la actualización y mantenimiento de la infraestructura de la red de la institución.
2. La CNPO supervisará la ejecución de la obra por parte de la empresa responsable y establecerá los estándares a implementar en la infraestructura de la red.
3. La CNPO deberá actualizar el libro de vida de la red una vez realizado cualquier cambio a la infraestructura de la misma.
4. Toda actualización de la infraestructura de la red debe cumplir con las normas de seguridad y estándares establecidos por la OCTSI.

PROCEDIMIENTO
ACTUALIZACIÓN DE INFRAESTRUCTURA DE RED

RESPONSABLE	ACCIÓN
COORDINACIÓN NACIONAL DE PRODUCCIÓN Y OPERACIONES	1. **Recibe** plano de distribución del espacio físico y oficio de requerimientos de componentes activos y pasivos de la red. 2. **Realiza** evaluación del espacio físico y requerimientos de componentes activos y pasivos de la red. 3. **Emite** informe indicando la cantidad de puntos de voz y datos y su ubicación física. 4. **Presenta** al comité técnico de control de cambios el informe de distribución de puntos y requerimientos de componentes activos y pasivos de la red.
COMITÉ TÉCNICO CONTROL DE CAMBIOS (CTCC)	5. **Recibe** de la CNPO la documentación señalada en el punto anterior. 6. **Discute** el informe de distribución de puntos y **requerimientos** de componentes activos y pasivos de la red. **6.1. En caso de no ser aprobado** el informe de distribución de puntos y requerimientos de componentes activos y pasivos de la red**,** realiza observaciones y devuelve el informe a la CNPO para su modificación. 7. **Aprueba** y entrega al Coordinador de la CNPO el **informe** de distribución de puntos y requerimientos de componentes activo y pasivos de la red.
COORDINACIÓN NACIONAL DE PRODUCCIÓN Y OPERACIONES	8. **Recibe** del CTCC el informe distribución de puntos y requerimientos de componentes activo y pasivos de la red aprobados y se realizó los pasos descritos en el procedimiento evaluación técnica para la adquisición de componentes activos y pasivos de la red, de este manual de normas y procedimientos. 9. **Recibe** del departamento de compras oficio indicando la empresa acreditada para la licitación. 10. **Concerta** reunión con la empresa acreditada. 11. **Gira** instrucciones para que la empresa comience con la realización de la obra. 12. **Supervisa** continuamente la ejecución de la obra, **verificando** que se cumpla con las normas ya establecidas.

NORMA
MANTENIMIENTO PREVENTIVO DE LOS COMPONENETES ACTIVOS Y PASIVOS DE LA RED

1. La CNPO será la única responsable del mantenimiento preventivo de los componentes activos y pasivos de la red con base en los planes establecidos.
2. La CNPO deberá informar con cuarenta y ocho (48) horas de anticipación el día y hora planificada para dar mantenimiento a los componentes, de ser requerida la suspensión del servicio de red.
3. El mantenimiento preventivo de los componentes activos y pasivos de la red deberá realizarse mensualmente.
4. La CNPO deberá exigir a las empresas la correcta ejecución de los contratos de mantenimiento adquiridos.
5. El mantenimiento preventivo se deberá realizar tanto a nivel de hardware como de software.

PROCEDIMIENTO
MANTENIMIENTO PREVENTIVO DE LOS COMPONENETES ACTIVOS Y PASIVOS DE LA RED

RESPONSABLE	ACCIÓN
COORDINACIÓN NACIONAL DE PRODUCCIÓN Y OPERACIONES	**1. Ejecuta** plan de mantenimiento preventivo de los componentes activos y pasivos de la red.
	2. Apertura ticket en el sistema Helpdesk interno con el fin de asignar la tarea al analista.
ANALISTA	**3. Consulta** a través del sistema Helpdesk interno la asignación.
	4. Revisa la situación de cada uno de los componentes activos y pasivos de la red especificados en el plan.
	5. Realiza el mantenimiento de los componentes tanto activos como pasivos, de acuerdo a los instructivos establecidos.
	6. Verifica que todos los servicios estén en funcionamiento.
	6.1En caso de no estar en funcionamiento todos los servicios procede de acuerdo con lo dispuesto en el procedimiento de atención a fallas de componentes activos y pasivos de la red descrito en este manual de normas y procedimientos.
	7. Elabora informe sobre los resultados del plan y entrega al CNPO.
	8. Documenta el ticket en el sistema Helpdesk y envía al Coordinador Nacional de Producción y Operaciones, así como el informe de resultados.
COORDINACIÓN NACIONAL DE PRODUCCIÓN Y OPERACIONES	**9. Recibe** informe sobre los resultados del mantenimiento preventivo de los responsables de efectuar el mantenimiento preventivo.
	10. Entrega informe de resultado del mantenimiento preventivo al Director de la OCTSI.

NORMA
AUDITORIA DE COMPONENTES ACTIVOS Y PASIVOS DE LA RED

1. La CNPO tiene la responsabilidad de realizar auditoría a una muestra de los elementos activos y pasivos de la red, con el fin de identificar cambios no autorizados.
2. El estado de los elementos activos y pasivos de la red deben coincidir con la información registrada en el libro de vida de la red, en el caso de que no coincida se debe restaurar al último estado registrado en el libro de vida de la red.
3. Cualquier cambio autorizado que se realice a los elementos activos y pasivos de la red, la CNPO debe actualizar el documento base e informa tanto al Director de OCTSI como a los demás administradores sobre los cambios realizados.
4. La CNPO debe elaborar el plan de auditoría de los elementos activos y pasivos de la red, de acuerdo con el resultado obtenido del monitoreo de la red, con el fin de garantizar el buen funcionamiento de la misma.

PROCEDIMIENTO
AUDITORIA DE COMPONENTES ACTIVOS Y PASIVOS DE LA RED

RESPONSABLE	ACCIÓN
COORDINACIÓN NACIONAL DE PRODUCCIÓN Y OPERACIONES	**1. Elabora** plan de auditoría de los componentes activos y pasivos de la red de acuerdo con los resultados obtenidos del monitoreo de la red. **2. Asigna** al responsable a través del sistema Helpdesk para que efectué la auditoría a los componentes activos y pasivos de la red.
ANALISTA	**3. Consulta** a través del Helpdesk la asignación. **4. Inicia** el proceso de auditoría a los componentes activos y pasivos de la red seleccionada. **5. Chequea** a través del documento base si existe algún cambio en la configuración de los componentes activos y pasivos de la red**.** o **Si existen cambios** restaura los componentes activos y pasivos de la red, de acuerdo con lo indicado en el documento base. **6. Efectúa** las pruebas para comprobar que los elementos activos y pasivos de la red estén de acuerdo con lo indicado en el documento base. o **Si no están de acuerdo al documento base** regresa al paso No.5 (cinco) de este procedimiento. **7. Elabora** Informe sobre el resultado de la auditoría y entrega al CNPO. **8. Documenta** el ticket en el sistema Helpdesk, **indicando** los cambios realizados en los componentes activos y pasivos de la red.
COORDINACIÓN NACIONAL DE PRODUCCIÓN Y OPERACIONES	**9. Recibe** el informe donde se indica el resultado de las auditorías realizadas. **10. Consulta** a través del sistema Helpdesk la respuesta de la asignación del operador y envía a la OCTSI.

Se puede evidenciar, que se contemplaron los tres elementos previstos por Sanz en la concepción del Plan de Seguridad Informática como lo son: Las políticas de seguridad, las normas y los procedimientos, siendo estas dos últimas colocadas solo cuatro a modo de referencia.

- Continuando con la norma exige recopilar los documentos de seguridad existentes en la organización: La única documentación existente para la fecha en la que se cubrió esta etapa se muestra en el (Anexo "I"), la cual fue dada por la dirección de TSI.

3.1.3. Evaluación de Riesgos: Durante esta fase se llevó a cabo una revisión de todas las brechas de seguridad potenciales, que afectan a la información sensible de la organización. El nivel de complejidad de este análisis fue proporcional a la naturaleza y valor de los activos, así como a los riesgos a los que esos activos están expuestos. El objetivo final de la evaluación de riesgos fue realizar un cálculo de los riesgos de los activos de información, con vistas a seleccionar los controles ISO/IEC 17799 adecuados para mitigar ese riesgo.

- Definición de una metodología para la clasificación de los riesgos: La metodología de las elipses es la que se usó en esta etapa, propuesta por Alexander (2.006) .
- Creación de un inventario de activos: Se realizó el inventario tanto de hardware como de servicios de información. Para el inventario de la red se utilizó una herramienta informática "NetViz" ver (Anexo "J"). Para el inventario de servicios se diseño una hoja de cálculo y se presenta el modelo en (Anexo "K"). Se realiza en el cuadro 25 resumen de los inventarios de activos.

Cuadro 25
Inventario de activos

Activos de información	Cantidad
Hardware	164
Software	40
Documentación	12
TOTAL	216

Nota: Autor (2006).

- Identificación y tasación de activos: La identificación se elaboró mediante el análisis del gráfico 15 a través de las elipses. La tasación se realizó en función de su impacto a su confidencialidad, integridad y disponibilidad con una escala cualitativa entre Alto (A), Medio (M) y Bajo (B). En el cuadro 26 se realiza un resumen de todos los activos a los que se le realizó tasación en la sede Rectoral y en el cuadro 27, por la sensibilidad de la información se muestra en forma detallada a modo de ejemplo la Tasación del SAI.

Cuadro 26
Tasación de activos

Activos de información	A	M	B
Hardware	22	39	103
Software	13	2	25
Documentación	1	0	11
TOTAL	36	41	139

Nota: Autor (2006).

- Identificación de requerimientos de seguridad: Estos son los contemplados una vez realizada la tasación. Son los que dieron como resultado Alto (A) en la columna "Total" de tasación, identificados en el cuadro 27.
- Evaluación de la posibilidad de que las amenazas y vulnerabilidades ocurran. Esto se llevó a cabo a través de la

técnica de lluvia de ideas[14] aplicada al personal involucrado en los procesos. Estos son mostrados en el cuadro 27.

- Cálculo de los riesgos de seguridad: Esto fue establecido haciendo el promedio del "Valor Activo" y la "Posible Ocurrencia" dando como resultado "Total General" identificados en el cuadro 27.

Cuadro 27
Realización del análisis y evaluación del riesgo.

Activos	Tasación			Total	Amenazas	Posibilidad de Ocurrencia	Vulnerabilidad	Posible explotación de vulnerabilidad	Valor Activo	Posible ocurrencia	Total General
	Confidencialidad	Integridad	Disponibilidad								
1. Datos	A	A	A	A	Error de usuario	B	Mal entrenamiento	B	A	M	M
					Escapes de Información	B	Acceso no autorizado	A			
					Alteración de la Información	M	Desconocimiento	B			
					Acceso no autorizado	M	Falta mecanismos de Autenticación	A			
					Destrucción de la información	M	Falta de políticas	A			
2. Software	A	A	A	A	Error de código	M	Personal no calificado	A	A	A	A
					Código Maliciosos	M	Control de acceso	A			
					Fallas técnicas	A	Energía eléctrica	A			
					Falta de seguridad	A	Falta de políticas	A			
3. Medio de comunicación	A	A	A	A	Fallas de funcionamiento	A	Energía eléctrica	A	A	A	A
					Falta de personal	A	Poca disponibilidad	A			
					Falta de seguridad	M	Errores de configuración	A			

Nota: Autor (2006).

[14] Lluvia de Ideas: Es una técnica grupal que permite la libre expresión del pensamiento e ideas de los participantes sin restricciones y limitaciones, a objeto de producir el mayor número de opiniones, datos, testimonios, alternativas y soluciones sobre un tema o problema. http://formacionenlinea.edu.ve

3.1.4. Tratamiento de Riesgos: A partir del informe de evaluación de riesgos se procedió a examinar cual era el tratamiento más adecuado para cada uno de los riesgos que se habían identificado.

- Selección de opciones de tratamiento de riesgos apropiadas: Siguiendo la cláusula 4.2.1 de la norma ISO/IEC 27001:2005 la cual plantea de forma muy precisa "se deben seleccionar objetivos de control y controles apropiados...". Es importante destacar, que el conjunto de decisiones tomadas con cada activo de información, como consecuencia de la evaluación del riesgo, se definió como "tratamiento del riesgo". El ISO/IEC guía 73:2002 Risk management – vocabulary guidelines for use estandards, lo define "como el proceso de selección e implementación de medidas para modificar el riesgo". Para esta selección se tomó los activos de información que presentaron un valor final de Alto (A) en la columna "Total General" identificados en el cuadro 27.
- Selección de controles para reducir el riesgo a nivel aceptable: En la cláusula 4.2.1. (h) de la norma ISO/IEC 27001:2005 se exige que se documente un "enunciado de aplicabilidad" y la clausula 4.3.1. (g) se hace mención también al enunciado de aplicabilidad, considerándolo un documento importante del SGSI. El enunciado de aplicabilidad es un documento en el cual deben registrarse los objetivos de control y los controles seleccionados, así como las razones para su selección. En el cuadro 28 se muestra el enunciado de aplicabilidad para reducir el riesgo a nivel aceptable para los activos seleccionados en relación al SAI. Es importante resaltar que en el cuadro 28 se colocó la descripción de los objetivos de control y controles, hecho para aclarar al lector, sin ser necesario en la metodología.

Cuadro 28
Enunciado de aplicabilidad

Activo de Información	Objetivo de control	Control	Justificación
Software	A.5.1 Política de seguridad de información	A.5.1.1 Documentar política de seguridad de información	Documentar las políticas de seguridad
	A.6.1 Organización interna	A.6.1.1 Compromiso de la gerencia con la seguridad de la información A.6.1.3 Asignación de responsabilidades de la seguridad de la información A.6.1.6 Contacto con autoridades	Minimizar errores humanos y mantener relaciones interinstitucionales
	A.7.1 Responsabilidad por los activos	A.7.1.1Inventarios de activos A.7.1.3 Uso aceptable de los activos	evitar perdida de activos e interrupción del servicio
	A.8.2 Durante el empleo	A.8.2.2 Capacitación y educación en seguridad de la información A.8.2.3 Proceso disciplinario	Minimizar los incidentes de seguridad y aprender de ellos
	A.9.1 Áreas seguras	A.9.1.1 perímetro de seguridad física A.9.1.2 Controles de entrada físicos A.9.1.4 Protección contra amenazas externas y ambientales	Evitar el acceso físico no autorizado
	A.11.2 Gestión del acceso del usuario	A.11.2.1 Inscripción del usuario A.11.2.2 Gestión de privilegios A.11.2.3 Gestión de la clave del usuario	Control de acceso a la información
	A.11.3 Responsabilidades del usuario	A.11.3.1 Uso de clave A.11.3.2 Equipo de usuario desatendido	Evitar el acceso no autorizado a la computadora
Medios de comunicación	A.6.1. Organización interna	A.6.1.1 Compromiso de la gerencia con la seguridad de la información A.6.1.3 Asignación de responsabilidades de la seguridad de la información	Proporcionar direccionalidad en la seguridad y evitar errores humanos
	A.7.1 Responsabilidad por los activos	A.7.1.1 Inventarios de activos A.7.1.3 Uso aceptable de los activos	evitar perdida de activos e interrupción del servicio
	A.8.2 Durante el empleo	A.8.2.2 Capacitación y educación en seguridad de la información A.8.2.3 Proceso disciplinario	Minimizar los incidentes de seguridad y aprender de ellos
	A.12.2 Procesamiento correcto en las aplicaciones	A.12.2.1 Validación de data de Insumo A.12.2.2 Control de procesamiento interno A.12.2.3 Integridad del mensaje	Asegurar la operación correcta de los medios de procesamiento de información.

Nota: Autor (2006).

CAPITULO V

EJECUCION Y EVALUACIÓN DE LA PROPUESTA

> "En todos los asuntos humanos hay esfuerzos, y hay resultados, y la fortaleza del esfuerzo es la medida del resultado."
>
> ***James Allen***

En este capítulo se describen los resultados de haber ejecutado y evaluado el plan de seguridad diseñado en el capítulo III a través de la fase IV. Es importante resaltar que el Manual para la Elaboración del Trabajo Conducente a Grado Académico de Especialización, Maestría y Doctorado de la UCLA (2.002) refiere al respecto "La fase IV es la ejecución y evaluación de la propuesta. Esta fase no es obligatoria para los aspirantes a especialistas o magíster pero si para los doctores".

Fase IV: Evaluación del diseño del Plan de Seguridad Informática

Para evaluar la efectividad del diseño propuesto en la fase III se requirió de la implantación y Operación del Plan de Seguridad Informática, el cual se referencia en el cuadro 29.

Cuadro 29
Implantación y Operación

4.1. Implantación y Operación (Do)	
4.1.1. Formación y sensibilización	● Impartir formación entre los empleados sobre lo nuevos procedimientos que se van a implantar. ● Concienciar a la plantilla de la importancia que el proyecto de seguridad tiene para la Organización
4.1.2. Implantación del SGSI	● Implantar el plan de tratamiento de riesgos. ● Implantar políticas y procedimientos del SGSI. ● Implantar los controles seleccionados.

Nota: Autor (2006).

4.1. Implantación y Operación (Do)

4.1.1. Formación y sensibilización: Los empleados son el eslabón más débil en la seguridad de la información de la organización, por eso es muy importante establecer un programa de concienciación de la seguridad de la información entre el personal.

- Impartir formación entre los empleados sobre lo nuevos procedimientos que se van a implantar: En un principio se dictó inducción al personal. Para visualizar el alcance de las medidas que se adoptaron, en el (Anexo "L") se coloca la memoria fotográfica del caso. Seguidamente se adiestró al personal usuario sobre el uso de la plataforma tecnológica con los cambios realizados en el área de seguridad, procurando un mínimo de impacto al usuario final.
- Concienciar a la plantilla de la importancia que el proyecto de seguridad tiene para la Organización: En este sentido, se ha mantenido una estrecha relación con la directiva de la Universidad a fin de expresar la importancia de invertir en el área de tecnología y en especial en el área de seguridad de la información. Los resultados de esta iniciativa es la asignación de recursos para la ejecución de proyectos, indicados en la fase II Factibilidad.

4.1.2. Implantación del SGSI.

- Implantar el plan de tratamiento de riesgos: Este es un documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. Para el Tratamiento del Riesgo existen cuatro estrategias, que son las más difundidas a nivel

internacional. A continuación se hará una breve descripción de cada una de ellas:

- Reducción del Riesgo: Para los riesgos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente identificados por la empresa. Los controles deben obtenerse del anexo "A" del ISO 27001:2005. Los controles escogidos y los objetivos de control respectivos deben estar documentados en el denominado "enunciado de aplicabilidad", tal como se detalla en la cláusula 4.2.1 (4) (j) del estándar. (ISO/IEC 27001:2005).
- Aceptación del Riesgo: En muchas ocasiones a la empresa se le presentan circunstancias donde no se pueden encontrar controles ni tampoco es factible diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.
- Transferencia del Riesgo: La transferencia del riesgo, es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En estas circunstancias podría ser económicamente viable, transferir el riesgo a una aseguradora.
- Evitar el Riesgo: La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

En la presente investigación se decidió por la primera opción, la cual se desarrollo en el cuadro 28 “Enunciado de aplicabilidad”.

- Implantar políticas y procedimientos del SGSI: En este sentido se implementó las políticas y procedimientos indicados en la Fase III del diseño del Plan de Seguridad Informática.
- Implantar los controles seleccionados: Una vez determinado los elementos ya descritos, se procede a realizar la implementación para cada uno de los controles indicados en el enunciado de aplicabilidad. En tal sentido y como desarrollo académico se muestra el cuadro 30 Implantación de los controles. Es importante resaltar que en el cuadro 30 se colocó la descripción de los objetivos de control y controles, hecho para aclarar al lector, sin ser necesario en la metodología.

Cuadro 30
Implantación de los controles

Activo de Información	Objetivo de control	Control	Implementación
Software	A.5.1Política de seguridad de información	A.5.1.1 Documentar política de seguridad de información	● Descritas en la Fase III del diseño del Plan de Seguridad Informático.
	A.6.1 Organización interna	A.6.1.1 Compromiso de la gerencia con la seguridad de la información A.6.1.3 Asignación de responsabilidades de la seguridad de la información A.6.1.6 Contacto con autoridades	● Aprobación del Reglamento de Tecnología y Servicios de Información ● Funciones detalladas en el Reglamento de TSI. "http://www.unexpo.edu.ve/documentos/05-E09-05.pdf" ● Ingreso al comité técnico de Reacciun[15], Fundacite[16], ministerio de ciencia y tecnología.
	A.7.1 Responsabilidad por los activos	A.7.1.1 Inventarios de activos A.7.1.3 Uso aceptable de los activos	● Ver anexo "J" y anexo "K" ● Descritas en la Fase III del diseño del Plan de Seguridad Informático.
	A.8.2 Durante el empleo	A.8.2.2 Capacitación y educación en seguridad de la información A.8.2.3 Proceso disciplinario	● El Coordinador Nacional de Tecnología de Información recibió adiestramiento en "Auditoría en Sistemas de Gestión de Seguridad de la Información" dictado por Fondonorma[17]; "Fundamentos de seguridad en redes de datos" dictado por la Universidad Centrooccidental Lisandro Alvarado (UCLA), esto con el fin de servir de multiplicador de los adiestramientos recibidos al personal asignado al área de seguridad dentro de la institución. ● El proceso disciplinario se puede observar en la Fase III del diseño del Plan de Seguridad Informático.
	A.9.1 Áreas seguras	A.9.1.1 perímetro de seguridad física A.9.1.2 Controles de entrada físicos A.9.1.4 Protección contra amenazas externas y ambientales	● Se implementó perímetros de seguridad tales como paredes y puertas de ingreso controlado para proteger áreas que contienen información y medios de procesamiento de información "Cuarto de cableado principal y servidores" (CCPS). ● Sólo se permite acceso al CCPS al personal autorizado. ● Se tiene protección física contra daño por fuego, inundación, y disturbios civiles dentro del CCPS.
	A.11.2 Gestión del acceso del usuario	A.11.2.1 Inscripción del usuario A.11.2.2 Gestión de privilegios A.11.2.3 Gestión de la clave del usuario	● Se elaboraron Normas y procedimientos, se puede observar en la Fase III del diseño del Plan de Seguridad Informático.
	A.11.3 Responsabilidades del usuario	A.11.3.1 Uso de clave A.11.3.2 Equipo de usuario desatendido	● Se instaló una infraestructura de control de dominio de software privativo "Windows 2003 Server" Active Directory del cual se crearon perfiles de usuario que se describen en el Anexo "M". ● Se puede observar en la Fase III del diseño del Plan de Seguridad Informático.

Nota: Autor (2006).

[15] REACCIUN: REd ACadémica de Centros de Investigación y Universidades Nacionales. http://www.reacciun2.edu.ve/view/reacciun.php

[16] FUNDACITE: FUNdación para el Desarrollo de lA CIencia y la Tecnología. http://www.fundacite.lara.gov.ve/

[17] FONDONORMA: es una Asociación Civil, sin fines de lucro, con personalidad jurídica y patrimonio propio, creada en septiembre de 1973 para promover las actividades de Normalización y Certificación de la Calidad con la intención de estimular la competitividad del sector productivo venezolano. http://www.fondonorma.org.ve/

La última etapa de la fase IV del capítulo V, muestra como se evaluó el diseño del Plan de Seguridad Informática en función del modelo PDCA, establecido como marco de referencia de la norma ISO/IEC 27001:2005. En este sentido, el cuadro 31 se detalla a continuación:

Cuadro 31
Evaluación del plan de seguridad

4.2. Monitorización y Revisión (Check)	
4.2.1. Monitorización del SGSI	● Ejecutar procedimientos de monitorización para detectar errores de proceso, identificar fallos de seguridad de forma rápida y acciones a realizar.
4.2.2. Revisión del SGSI: (Se propone como elemento para futuras investigaciones y en este sentido, se deja una guía de como debe ejecutarse).	● Revisiones periódicas de la política y alcance del SGSI, así como de su eficacia. Auditorías internas/externas del SGSI

Nota: Autor (2006).

4.2. Monitorización y Revisión (Check)

4.2.1. Monitorización del SGSI

- Ejecutar procedimientos de monitorización para detectar errores de proceso, identificar fallos de seguridad de forma rápida y acciones a realizar: En concordancia con lo establecido McNab (2.004) propone una metodología para la evaluación de seguridad de redes basado en los estándares más importantes de los Estados Unidos y para el Reino Unido específicamente "National Security Agency's INFOSEC Assessment Methodology (NSA IAM)"[18] y "Communications and Electronics Security Gruop (CESG CHECK)"[19] respectivamente.

[18] http://www.iatrp.com
[19] http://www.cesg.gov.uk

La NSA IAM propone un entorno de trabajo definido en tres niveles de evaluación relacionado con el testeo de redes informáticas basadas en IP:

1. Evaluación: Este nivel implica realizar una descripción con la cooperación de la organización, incluyendo acceso a su documentación de políticas, procedimientos, etc.
2. Valoración: Es un proceso práctico que implica la realización de pruebas con herramientas de exploración y penetración de redes, usando conocimientos técnicos específicos y con consentimiento de la institución.
3. Equipo Rojo: Es un una evaluación sin la cooperación de la institución de carácter externo a la red objeto de la penetración, e implica pruebas de penetración.

La CESG CHECK del mismo modo permite proporcionar servicios de evaluación en seguridad cubriendo aspectos como políticas, procedimientos, etc. Ambas metodologías serán abordados, a fin de proporcionar un refinado resultado de la evaluación del Diseño del Plan de Seguridad de Información implementado en la Institución. En este sentido, se puede inferir que existen en estas metodologías de evaluación dos grandes áreas: ***la técnica*** desarrollada en este punto utilizando el nivel de "Equipo Rojo" de la NSA IAM, descrita en el gráfico 16 y para cuyas acciones se utilizaron las herramientas identificadas en el (Anexo "N") y ***la gerencial*** propuesta en el punto 4.2.2., Revisión del SGSI la cual podría estar basada en CESG CHECK es futuras investigaciones.

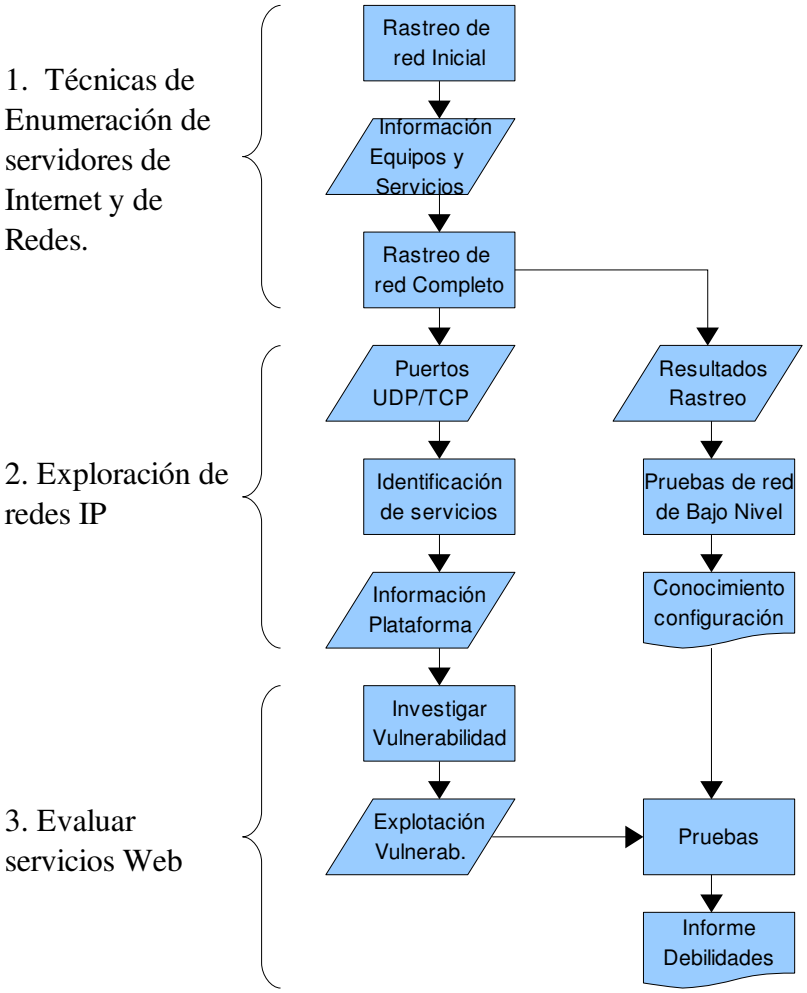


Gráfico 16. Diagrama de flujo para la evaluación de la seguridad en redes.
Nota: McNab (2004).

El gráfico 16 muestra el diagrama de flujo para evaluar la seguridad en redes, dando como resultado los análisis descritos en los cuadros siguientes. La evaluación técnica se ejecutó en dos momentos distintos, uno antes de aplicar el plan de seguridad informático (2do. semestre 2.005) y otra después de aplicarlo (1er. semestre 2.007), con el objeto de medir estadísticamente las mejoras obtenidas.

a. Técnicas de Enumeración de servidores de Internet y de Redes.

Se trata de recorrer las opciones basadas en Internet que un potencial atacante tiene que obtener de la red objetivo, desde la búsquedas Web abiertas hasta el rastreo y solicitud de servidores DNS con autentificación. Se detallan algunas de las herramientas utilizadas: Sam Spade Windows, nslookup, host, dig, etc.

Enumerar detalles de contactos.

Cuadro 32
Enumerar detalles de contactos Unexpo

ítem	Antes de aplicar el Plan	Después de aplicar el Plan	% Mejora Cuantitativamente
Enumeración	36	14	61%

Nota: Autor (2007).

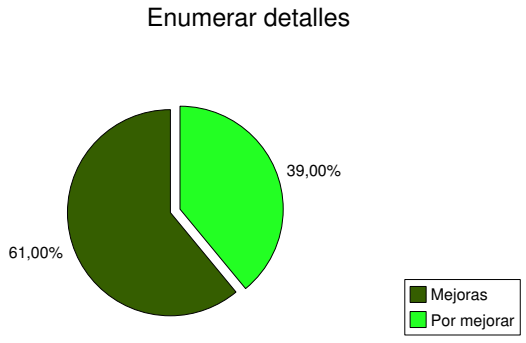


Gráfico 17. Enumerar detalles Unexpo
Nota: Resultado de la ejecución de enumerar detalles

En el gráfico 17, se muestra una mejora del sesenta y uno por ciento (61%) con respecto a la situación encontrada al comienzo de la investigación, hecho que refleja positivamente la ejecución del plan de seguridad.

Consulta Network Informations Centers (NIC) y DNS

Cuadro 33
NIC Unexpo

ítem	Antes de aplicar el Plan	Después de aplicar el Plan	% Mejora Cuantitativamente
Cantidad de DNS Activos	1	2	50%

Nota: Autor (2007).

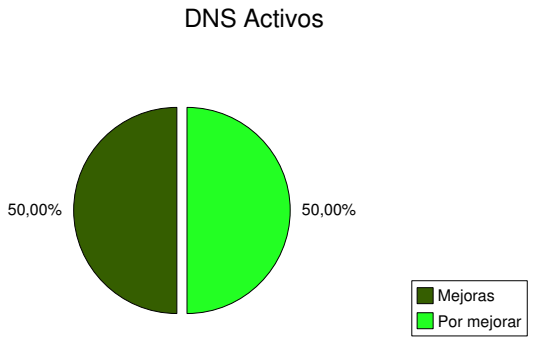


Gráfico 18. DNS Activos Unexpo
Nota: Resultado de la ejecución de enumerar detalles

En el gráfico 18, se muestra una mejora del cincuenta por ciento (50%) con respecto a la situación encontrada al comienzo de la investigación.

Cuadro 34
DNS Unexpo

ítem	Antes de aplicar el Plan	Después de aplicar el Plan		% Mejora Cuantitativamente
DNS (Equipo)	"A"	"A"	"B"	
Serial Sync	Ok	Ok	Ok	100%
Autoridad	Ok	Ok	Ok	100%
Recursividad	1	1	1	0%
Soporte TCP	2	Ok	Ok	100%
			Total	75%

Nota: Autor (2007).

Cuadro 35
Tabla leyenda DNS

No.	Leyenda	Observación
0	Ok	En perfectas condiciones.
1	Con recursividad	Corresponde a un error grave. Un servidor autoritativo no debe ser recursivo, pues está sujeto a ataques de Cache Poisoning. Dicho ataque consiste en alterar la información entregada por el DNS mediante respuestas inválidas, pues un servidor recursivo averigua y memoriza las respuestas que recibe.
2	Error consultando vía TCP	El RFC 1035 indica que un servidor de DNS debe soportar consultas vía UDP y TCP. Aunque en general se prefiere UDP, TCP se utiliza para las transferencias de zona y para contestar consultas cuya respuesta excede los 512 bytes. (Mayores referencias en la sección 4.2 y 4.2.2 del RFC ya mencionado).
3	Servidor no Disponible	Es un error grave, porque implica que un servidor de nombres delegado no es alcanzable por diferentes razones: No resuelve número IP, no contesta válidamente, no es alcanzable a nivel de la red. Esto puede producir errores temporales de resolución.

Nota: Autor (2007).

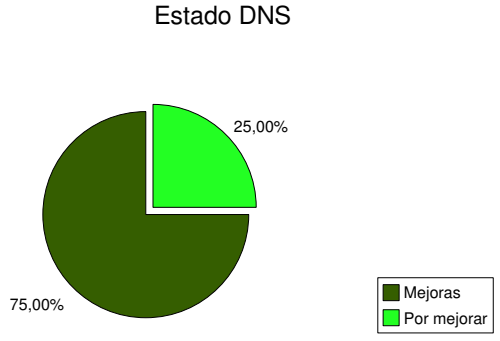


Gráfico 19. Estado DNS Unexpo
Nota: Resultado de la ejecución de enumerar detalles

En el gráfico 19, se muestra una mejora del setenta y cinco por ciento (75%) con respecto a la situación encontrada al comienzo de la investigación.

b. Exploración de redes IP

Se trata de todas las técnicas conocidas de exploración de puertos TCP, UDP en redes IP y sus aplicaciones más relevantes. También se trata de técnicas de evasión de IDS y del análisis de bajo nivel de paquetes. Se detallan algunas de las herramientas utilizadas: nmap, wget, scanudp, fragrouter, hping2, etc.

Cuadro 36
Exploración de redes IP Unexpo

Servidores públicos DMZ[20]	Antes de aplicar el Plan	Después de aplicar el Plan	% Mejora Cuantitativamente
Responde a Rastreo ICMP[21]	Si	No	100%
Abre puertos TCP[22] necesarios	No	Si	100%
Abre puertos UDP[23] necesarios	No	Si	100%
		Total	100%

Nota: Autor (2007).

[20] DMZ: Demilitarized zone o Zona DesMilitarizada. En seguridad informática, una zona desmilitarizada (DMZ) o red perimetral es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet. http://es.wikipedia.org/wiki/Zona_desmilitarizada

[21] ICMP: Protocolo de Control de Mensajes de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el subprotocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP). http://es.wikipedia.org/wiki/Internet_Control_Message_Protocol

[22] TCP: Protocolo de Control de Transmisión (TCP en sus siglas en inglés, Transmission Control Protocol que fue creado entre los años 1973 - 1974 por Vint Cerf y Robert Kahn) es uno de los protocolos fundamentales en Internet. http://es.wikipedia.org/wiki/Transmission_Control_Protocol

[23] UDP: Protocolo de Datagrama de Usuario (en inglés *User Datagram Protocol*) un protocolo sin conexión que, como TCP, funciona en redes IP. http://www.masadelante.com/faq-udp.htm

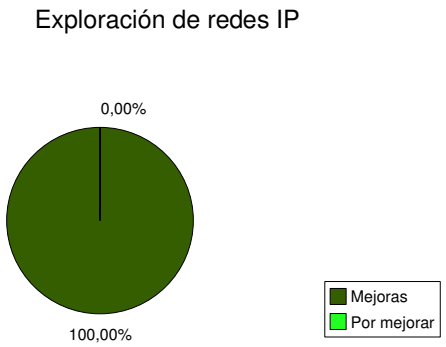


Gráfico 20. Exploración de redes IP Unexpo
Nota: Resultado de la Exploración de redes IP

En el gráfico 20, se muestra una mejora total del cien por ciento (100%) con respecto a la situación encontrada al comienzo de la investigación.

c. Evaluar servicios Web

Se trata de la evaluación de vulnerabilidades y errores de servicios Web como: IIS, apache, OpenSSL y otros componentes como Frontpage, extensiones, etc. Se detallan algunas de las herramientas utilizadas: telnet, webserverfp, nikto, n-stelth, etc.

Cuadro 37
Evaluar servicios Web Unexpo

ítem	Antes de aplicar el Plan	Después de aplicar el Plan	% Mejora Cuantitativamente
Vulnerabilidades	32	7	78%
Errores	54	19	64%
		Total	71%

Nota: Autor (2007).

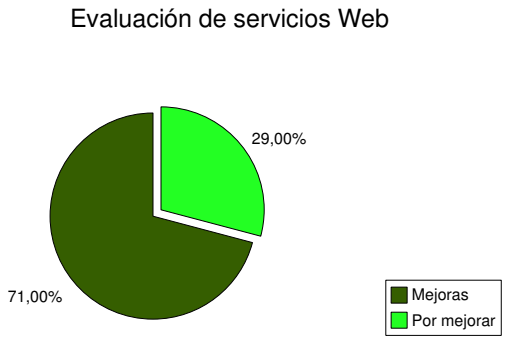


Gráfico 21. Evaluación de servicios Web Unexpo
Nota: Resultado de la Exploración de redes IP

En el gráfico 21, se muestra una mejora del setenta y uno por ciento (71%) con respecto a la situación encontrada al comienzo de la investigación.

Al finalizar la evaluación de seguridad realizada en la institución se obtuvo una mejora total del setenta y uno por ciento (71%) en los aspectos de enumeración de servidores de Internet y de redes; exploración de redes IP y servicios Web. Este hecho refleja positivamente la ejecución del Plan de Seguridad Informática diseñado para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral, tomando como referencia la norma ISO/IEC-27001:2005 y la norma ISO/IEC-17799:2005.

Como elemento complementario se realiza una comparación desde el punto de vista cualitativo con otras universidades del país que se muestra en el (Anexo "O").

4.2.2. Revisión del SGSI: Elemento que se presenta como recomendación adicional a ser desarrollado en una futura investigación.

- Revisiones periódicas de la política y alcance del SGSI, así como de su eficacia. Auditorías internas/externas del SGSI. Tal y como se explicó en el punto 4.2.1, Monitorización del SGSI, el aspecto ***gerencial*** debería ser desarrollado en este apartado.

  En este sentido, la norma ISO/IEC-27001:2005 explica que la organización realizará auditorías internas al SGSI a intervalos planeados para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a esta norma y para analizar y planificar acciones de mejora. Ninguna persona podrá auditar su propio trabajo, ni cualquier otro que guarde relación con él.

  La responsabilidad y requerimientos para el planeamiento y la conducción de las actividades de auditoría, los informes resultantes y el mantenimiento de los registros será definido en un procedimiento.

  En este orden de ideas y tomando como base la norma ISO-19011:2002 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental", en concordancia con lo establecido el (Anexo "P") detalla: el programa de auditoría, el plan de auditoría, la lista de chequeo general, el cronograma de auditoría, la lista de chequeo específica y el reporte de no conformidad. Esto con el fin de que sea aplicada por los entes indicados a futuro.

Para culminar el capítulo V, en el (Anexo "Q") se identifican a modo descriptivo una pequeña muestra de las soluciones brindadas a lo largo de la investigación y en el (Anexo "R") el curriculum vitae del investigador.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

> "Dichoso el hombre que ha encontrado la sabiduría y el hombre que alcanza la prudencia; más vale su ganancia que la ganancia de la plata, su renta es mayor que la del oro."
>
> Proverbios 3, 13-14.

En atención a la aplicación de las técnicas e instrumentos de recolección de datos aplicadas en la Universidad, así como la metodología empleada para la evaluación de la seguridad de la información, se puede realizar las siguientes conclusiones, las cuales denotan grandes beneficios al aplicar el diseño propuesto. En tal sentido, se detalla de acuerdo a las fases ejecutadas en la investigación:

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

- El personal tiene escasos conocimientos en el área de seguridad de la información, así como de los estándares aplicados en la materia.
- No existen planes de sensibilidad en seguridad de la información dentro de la Universidad.
- Se desconoce las políticas de seguridad de información, el plan de continuidad del negocio y el plan de recuperación ante desastres.
- Todo el personal manifestó desconocer si existía un análisis de riesgo sobre los activos de información de la Universidad.
- Se demostró la hipótesis tacita especificada en el Capítulo I. "planteamiento del problema".

- Se realizó dos instrumentos de diagnósticos la “Entrevista” y el “Cuestionario”, los cuales fueron validados y demostrado su confiabilidad, pudiendo servir como apoyo a futuras investigaciones relacionadas con el tema.

Fase II. Factibilidad: Se demostró que existía factibilidad tanto operativa, técnica y económica para aplicar el plan de seguridad de información dentro de la Universidad.

Fase III. Diseño del plan de seguridad informática: se aplicó la norma ISO/IEC 27001:2005 y la norma ISO/IEC 17799:2005, para el diseño del Plan de Seguridad Informática.

Fase IV. Evaluación del diseño del Plan de Seguridad Informática: para evaluar la efectividad del diseño se implantó el plan y se utilizó una metodología para la evaluación de seguridad de redes basado en los estándares más importantes de los Estados Unidos como lo es: el NSA IAM y el CESG CHECK del Reino Unido. De los resultados obtenidos se puede inferir que:

Se obtuvo una mejora total del setenta y uno por ciento (71%), hecho que refleja positivamente la efectividad del diseño del Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica “Antonio José de Sucre” sede Rectoral. Todo esto como resultado de que se implementaron soluciones de seguridad basado en los dominios de la norma ISO/IEC 27001:2005, tales como: políticas de seguridad, políticas de respaldos, normas y procedimientos, inventario de activos de información, consolidación de dominio para la autenticación, definición de perfiles de usuarios, servidor de archivos, servidor de antivirus corporativo, servidor de actualizaciones de seguridad, servidor proxy, normalización de estaciones de trabajo, firewall, implementación de una red conmutada a través de VLAN, documentación e ingeniería de detalle de la red entre otros.

Como reflexión final se puede concluir con asertividad que la seguridad informática es un proceso continuo el cual estadísticamente se encuentra entre cero (0) y uno (1), sin lograr tocar en ningún momento el límite superior uno (1).

Recomendaciones

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

- Se recomienda, en primer lugar, aplicar el Plan de Seguridad Informática en todos los Vicerrectorados de la Universidad.
- Invertir en adiestramiento al personal de tecnología dirigido al fortalecimiento de las áreas críticas de servicios y seguridad.
- Difundir en la institución las políticas de seguridad de la información.
- Profundizar la difusión de una consciencia usuaria que permita aumentar la seguridad existente.
- Realizar un proyecto de análisis de riesgo de toda la Unexpo.
- Se debe desarrollar el Business Continuity Plan (BCP) o Plan de Continuidad del Negocio, así como también, el Business Impact Analysis (BIA) o Análisis de Impacto del Negocio.
- Se recomienda realizar una auditoría por una empresa certificadora a la UNEXPO, soportado por los documentos del (Anexo "P") que se listan a continuación: el programa de auditoría, el plan de auditoría, la lista de chequeo general, el cronograma de auditoría, la lista de chequeo específica y el reporte de no conformidad.
- Como recomendación final se ratifica la necesidad de implementar una solución de Cluster Server y configurar una solución de Infraestructura PKI, indicados en el (Anexo "Q") de la presente investigación.

BIBLIOGRAFÍA

Alexander, A (2.006). *Análisis del riesgo y el sistema de gestión de información: el enfoque ISO 27001:2005. [On-Line] Disponible en:* www.eficienciagerencial.com [consultado agosto 2006].

Ary, D. Y otros (1.985) *Introducción a la investigación.* ED.: Interamericana, México – México.

Ary, W. (1.996). *Metodología de la Investigación.* ED.:Ediciones Roalg. Madrid - España.

Balestrini, M. (1.998). *Cómo se elabora el Proyecto de Investigación en Venezuela.* ED.:Consultores Asociados, Servicio Editorial. Caracas - Venezuela.

Barrios, M. (2.004). *Manual de trabajos de grado de especialización y maestría y tesis doctórales.* ED.: Universidad Pedagógica Experimental Libertador, Caracas - Venezuela.

Bigelow, S. (2.003). *Localización de averías, reparación, mantenimiento y optimización de redes.* ED. McGraw-Hill, Madrid – España.

Cerini, M. y Prá, P (2.002). *Plan de seguridad informática. [On-Line] Disponible en:*http://www.segu-info.com.ar/tesis/, Trabajo de grado presentado para optar al título de Ingeniero en Sistemas. Universidad Católica de Córdoba. Córdoba – España. [consultado agosto 2.006].

Decreto 3.087 (Creación de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre"). (1.979, Febrero 20) Gaceta Oficial de la República de Venezuela, 28.958.

De Souza, C. (2.002) G*erencia de seguridad de información en sistemas de teletrabajo.*[On-Line] Disponible en: P2P Emule. Trabajo de grado presentado para optar al título de Magister en Ingeniería. Universidad Federal de Santa Catarina, Florianópolis – Brasil. [consultado Mayo 2.006]

González, A. (2.003) S*istema de administración de riesgos en tecnología informática* [On-Line] Disponible: en: http://www.gestiopolis.com/recursos/documentos/fulldocs/ger1/sistecinfor.htm [consultado agosto 2.006].

Gomez, J. (2.006). *Seguridad en GNU/Linux.* Todo Linux No. 60 año 5, ED.: Studio Press, Madrid – España.

Hamana, J. (2.003) *Elementos básicos para modelos de seguridad en organizaciones venezolanas.* Trabajo de grado presentado para optar al título de Magister en Gerencia de Sistemas, Universidad Metropolitana, Caracas – Venezuela.

Hernandez, R. y otros (1.996) *Metodología de la investigación.* ED.: McGraw-Hill Interamericana, S.A. México DF-México.

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

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).

ISO-19011:2002 - Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental.

ISO/IEC 27001:2005 – Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Organización Internacional de Estándares (ISO).

ISO/IEC 73:2002 Risk management – vocabulary guidelines for use estandards. Organización Internacional de Estándares (ISO)

La Academia Latinoamericana de Seguridad Informática (2.004). *Microsoft TechNet modulo de seguridad.* [On-Line] Disponible en: www.mslatam.com/latam/technet/cso/Html-ES/home.asp [consultado Junio 2.005].

Ley Especial Contra Delitos Informáticos promulgada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2.001 por la Asamblea Nacional, Caracas - Venezuela.

Ley Sobre Mensajes de Datos y Firmas Electrónicas promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2.001, por Decreto N° 1.024 – 10 de febrero de 2001, Caracas - Venezuela.

Ley Orgánica de Telecomunicaciones, promulgada 12 de junio de 2000 y publicada en Gaceta Oficial No.36.970. Caracas - Venezuela.

Lineamientos OECD para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad. (2.002). [On-Line] Disponible en:www.oecd.org. París – Francia [consultado Junio 2.006].

Maiwald, E. (2.005) *Fundamentos de Seguridad de Redes.* ED.: Mc.Graw Hill, 2da. Edición, México D.F. - México.

McNab, C. (2.004) *Seguridad de redes.* ED.: Anaya Multimedia, Madrid - España.

Melamed, S. y Ripepi, M. (2.002). *Diseño e implantación de una arquitectura integrada de protección para la plataforma de correo electrónico en una empresa de telecomunicaciones incluyendo tanto la intranet como extranet*. Trabajo de grado presentado para optar al título de Ingeniero de Sistemas, Universidad Metropolitana, Caracas – Venezuela.

Murillo, S. (2.001), *Diseño y Aplicación de un Sistema Integral de Seguridad Informática para la UDLA*. [On-Line] Disponible en: http://140.148.3.250/u_dl_a/servlet/mx.udlap.ict.tales.html.Block?Thesis=80&Type=T Trabajo de grado presentado para optar al título de Maestría en Ciencias con Especialidad en Ingeniería en Sistemas Computacionales, Universidad de las Américas, Puebla, México [consultado Diciembre 2.004].

Oficina de Planificación del Sector Universitario (2.006), [On-Line] Disponible en: http://www.cnu.gov.ve. [consultado Diciembre 2.006].

PandaLabs (2.006). Informe trimestral PandaLabs. [On-Line] Disponible en: http://www.pandasoftware.com/ [consultado Agosto 2.006].

Tanenbaum, A. (2.003). *Redes de computadoras.* ED.:Pearson, 4ta. Edición, Naulcapan de Juárez – México.

Real Academia Española (2.006) [On-Line] Disponible en: http://www.rae.es/ [consultado Julio 2.006].

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 2.004. 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.

RFC 1035 , Domain names - implementation and specification [On-Line] Disponible: en: http://www.faqs.org/rfcs/rfc1035.html [consultado Diciembre 2.006].

Sabino, C. (1.998). *El proceso de investigación*. ED.: Panapo. Caracas – Venezuela.

Sanz, A. (2.006) *Administración de sistemas informáticos.* [On-Line] Disponible en: Antonio_sanz@flashmail.com [consultado Junio 2.006].

Senn, J. (1.987). *Análisis y diseño de sistemas de información.* ED.: McGraw-Hill México DF-México.

Scott, G. (1.988). *Principios de Sistemas de Información.* ED.: McGraw-Hill, Naucalpan de Juárez – México.

Universidad Centroccidental "Lisandro Alvarado" (UCLA). (2.002). *Manual para la Elaboración del Trabajo Conducente al Grado Académico de: Especialización, Maestría y Doctorado.* Barquisimeto – Venezuela

Universidad Nacional de Colombia y esCERT Universidad Politécnica Catalunya (2.005). [On-Line] *Lista de estándares de seguridad internacionales* disponible en :http://www.seguridad0.com, [consultado Agosto 2.006].

Anexos

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 información Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.5.1.1	Documentar política de seguridad de información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
A,6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo*:* Manejar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia 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 ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.
A.6.1.4	Proceso de autorización para los medios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control 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 Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.
A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.

A.7 Gestión de activos		
A.7.1 ***Responsabilidad por los activos*** Objetivo*:* Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' de una parte designada de a organización.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
A.7.2 Clasificación de la información Objetivo: Asegurar que a información reciba un nivel de protección apropiado.		
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.
A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo Objetivo*:* Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
A.8.2 ***Durante el empleo*** Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
A.8.3 Terminación o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.

A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
A.9 Seguridad física y ambiental		
A.9.1 ***Áreas seguras***		
Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
A.9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
A.9.2 ***Seguridad del equipo***		
Objetivo*:* Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2	Servicios públicos	Control El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
A.9.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
A.9.2.4	Mantenimiento de equipo	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera-del-local	Control Se debe aplicar seguridad al equipo fuera-del-local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6	Eliminación seguro o re-uso del equipo	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.
A.9.2.7	Traslado de Propiedad	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.
A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operacionales		
Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	Control Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambio	Control Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
A.10.1.3	Segregación de deberes	Control Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la

		organización.
A.10.1.4	Separación de los medios de desarrollo y operacionales	Control Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
A.10.2 Gestión de la entrega del servicio de terceros Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.		
A.10.2.1	Entrega del servicio	Control Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	Control Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.
A.10.2.3	Manejar los cambios en los servicios de terceros	Control Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la re-evaluación de los riesgos.
A.10.3 Planeación y aceptación del sistema Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	Control Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2	Aceptación del sistema	Control Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
A.10.4 ***Protección contra software malicioso y código móvil*** Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado
A.10.5 Respaldo (back-up) Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1	Back-up o respaldo de la información	Control Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
A.10.6 ***Gestión de seguridad de redes*** Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	Control Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
A.10.7 Gestión de medios Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	Control Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Eliminación de medios	Control Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
A.10.7.3	Procedimientos de manejo de la información	Control Se deben establecer los procedimientos para el manejo y almacenaje de la información para

		proteger dicha información de una divulgación no autorizada o un mal uso.
A.10.7.4	Seguridad de documentación del sistema	Control Se debe proteger la documentación de un acceso no autorizado.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas de información y software	Control Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajes electrónicos	Control Se debe proteger adecuadamente los mensajes electrónicos.
A.10.8.5	Sistemas de información comercial	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.10.9 Servicios de comercio electrónico Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		
A.10.9.1	Comercio electrónico	Control Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.
A.10.9.2	Transacciones en-línea	Control Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o re-envío no-autorizado del mensaje.
A.10.9.3	Información disponible públicamente	Control Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	Registro de auditoría	Control Se deben producir registros de la actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2	Uso del sistema de monitoreo	Control Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3	Protección de la información del registro	Control Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
A.10.10.4	Registros del administrador y operador	Control Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.
A.10.10.6	Sincronización de relojes	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.
A.11 Control de acceso		
A.11.1 Requerimiento comercial para el control del acceso Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
A.11.2 Gestión del acceso del usuario Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.		

A.11.2.1	Inscripción del usuario	Control Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Se debe restringir y controlar la asignación y uso de los privilegios.
A.11.2.3	Gestión de la clave del usuario	Control La asignación de claves se debe controlar a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso del usuario	Control La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		
A.11.3.1	Uso de clave	Control Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2	Equipo de usuario desatendido	Control Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
A.11.3.3	Política de pantalla y escritorio limpio	Control Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
A.11.4 Control de acceso a redes Objetivo: Evitar el acceso no-autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	Control Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.11.4.2	Autenticación del usuario para conexiones externas	Control Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación del equipo en red	Control Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección del puerto de diagnóstico remoto	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Segregación en redes	Control Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
A.11.4.6	Control de conexión de redes	Control Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales (ver 11.1).
A.11.4.7	Control de 'routing' de redes	Control Se deben implementar controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema de operación Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	Control Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.
A.11.5.3	Sistema de gestión de claves	Control Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4	Uso de utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5	Sesión inactiva	Control Las sesiones inactivas deben cerrarse después de un período de inactividad definido.

A.11.5.6	Limitación de tiempo de conexión	Control Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a la aplicación e información Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
A.11.6.1	Restricción al acceso a la información	Control Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2	Aislamiento del sistema sensible	Control Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
A.11.7 Computación móvil y tele-trabajo Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.		
A.11.7.1	Computación móvil y comunicaciones	Control Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
A.11.7.2	Tele-trabajo	Control Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.12.1 Requerimientos de seguridad de los sistemas Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	Control Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de data de Insumo	Control El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2	Control de procesamiento interno	Control Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje	Control Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4	Validación de data de output	Control Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión clave	Control Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización.
A.12.4 Seguridad de los archivos del sistema Objetivo: Garantizar la seguridad de los archivos del sistema		
A.12.4.1	Control de software operacional	Control Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.4.2	Protección de la data de prueba del sistema	Control Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
A.12.4.3	Control de acceso al código fuente del programa	Control Se debe restringir el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo*:* Mantener la seguridad del software e información del sistema de aplicación		
A.12.5.1	Procedimientos de control de cambio	Control La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las	Control

	aplicaciones después de cambios en el sistema operativo	Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	Control No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
A.12.5.4	Filtración de información	Control Se deben evitar las oportunidades de filtraciones en la información.
A.12.5.5	Desarrollo de outsourced software	Control El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.
A.12.6 Gestión de vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
A. 13 Gestión de incidentes en la seguridad de la información		
A.13.1 Reporte de eventos y debilidades en la seguridad de la información Objetivo*:* Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
A.13.1.1	Reporte de eventos en la seguridad de la información	Control Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2	Reporte de debilidades en la seguridad	Control Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	Control Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
A.14 Gestión de la continuidad comercial		
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de continuidad comercial	Control Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2	Continuidad comercial y evaluación del riesgo	Control Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	Control Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.

A.l4.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	Control Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento con requerimientos legales Objetivo*:* Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
A.15.1.1	Identificación de legislación aplicable	Control Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
A.15.1.2	Derechos de propiedad intelectual (IPR)	Control Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3	Protección los registros organizacionales	Control Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
A.15.1.4	Protección de data y privacidad de información personal	Control Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
A.15.1.5	Prevención de mal uso de medios de procesamiento de información	Control Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
A.15.1.6	Regulación de controles criptográficos	Control Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.		
A.15.2.1	Cumplimiento con las políticas y estándares de seguridad	Control Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2	Chequeo de cumplimiento técnico	Control Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
A.15.3 Consideraciones de auditoría de los sistema de información Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoría de los sistema de información.		
A.15.3.1	Controles de auditoría de sistemas de información	Control Se deben planear cuidadosamente los requerimientos y actividades de las auditorías que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Anexo “B”. Gantt del Plan de Seguridad Informática.

Fase del Proyecto	Actividad	Sub Actividad	Tarea	1er. Trimestre	2do. Trimestre	3er. Trimestre	4to. Trimestre
I	1. Diagnóstico	1.1 Entrevista 1.2. Cuestionario 1.3. Observación directa	* Validez y confiabilidad de los instrumentos * Técnicas y presentación de resultados * Análisis de la entrevista * Análisis del cuestionario * Análisis observación directa				
II	2. Factibilidad	2.1. Operativa 2.2. Técnica 2.3. Económica					
III	3. Diseño del plan de seguridad informático	3.1 Establecimiento del SGSI	3.1.1. Inicio del Proyecto				
			3.1.2. Definición del SGSI				
			3.1.3. Evaluación de Riesgos				
			3.1.4. Tratamiento de Riesgos				
IV	4. Evaluación del plan de seguridad informático	4.1. Implantación y Operación	4.1.1. Formación y sensibilización				
			4.1.2. Implantación del SGSI				
		4.2. Monitorización y Revisión	4.2.1. Monitorización del SGSI				
			4.2.2. Revisión del SGSI (Propuesta)				

Anexo “C” Entrevista

GUIA DE ENTREVISTA PARA EL DIAGNOSTICO DE LA SITUACION ACTUAL EN REFERENCIA DE “DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA “ANTONIO JOSE DE SUCRE” SEDE RECTORAL”

ENTREVISTA

1. ¿Indique si la Universidad esta certificada en alguno de los estándares de seguridad de información e indicar de ser afirmativo el estándar, fecha de certificación y entidad certificadora?

2. ¿Conoce usted alguno de los estándares de seguridad de información y de ser afirmativo mencione como adquirió usted este conocimiento?

3. ¿Indique las clasificaciones de seguridad de información actualmente existentes en la Universidad?

4. ¿Indique el uso que se le da a la información según las clasificaciones existentes en la institución?

5. ¿Indique si la institución posee programas dirigidos a sensibilizar sobre la seguridad de la información para todos los empleados?

6. ¿Las políticas de seguridad son para toda la institución o solo para la dirección de tecnología?

7. ¿Existe un documento que reúne todas las políticas de seguridad de información vigentes?

8. ¿Existe un procedimiento para actualizar periódicamente el documento de políticas de seguridad?

9. ¿Existe un archivo de Seguridad de Información que reúne todos los convenios vigentes en este sentido?

10. ¿En su institución el plan de continuidad de operaciones cuando se definió o actualizó por última vez, indique si hizo algún simulacro en los últimos seis meses y cuales recomendaron en dicha oportunidad acciones urgentes a realizar para reducir riesgos?

11. ¿En la institución indique cual es el plan de recuperación ante desastres que se tiene y si hizo algún simulacro en los últimos seis meses e indique cuales recomendaciones se realizaron en dicha oportunidad para reducir el riesgos?

12. ¿En la institución han realizado en alguna oportunidad una evaluación de riesgos de la información?

13. ¿En la institución han realizado una evaluación de vulnerabilidades de la red y de ser afirmativo ha sido en los últimos seis meses?.

14. ¿En la institución han realizado pruebas de penetración perimetral y de ser afirmativo se recomendaron en dicha oportunidad acciones urgentes a realizar para reducir riesgos?

15. ¿En su institución tienen software antivirus y de ser afirmativo indique la fecha de su última actualización.?

16. ¿En su institución tienen software para detección de intrusos?

Anexo "D" Cuestionario

CUESTIONARIO

La presente tiene como finalidad conocer su opinión con respecto a la seguridad de la información. como parte de un estudio para la realización de la tesis titulada "**DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA "ANTONIO JOSE DE SUCRE" SEDE RECTORAL"**

Instrucciones:

6.Lea cuidadosamente cada una de las preguntas antes de responder.
7.Todas deben ser respondidas.
8.Al responder, coloque una equis (X) debajo de la alternativa que usted considere correcta, solo deben considerar una como correcta.

Es importante que se asegure de haber contestado todas las preguntas, espontáneamente y con veracidad...

Se le Agradece su apoyo y colaboración...

PREGUNTAS:

1. ¿Considera usted que la Universidad tiene certificación en alguno de los estándares de seguridad de información?

Totalmente en Desacuerdo	*En Desacuerdo*	*Indeciso*	*De Acuerdo*	*Totalmente De Acuerdo*
☐	☐	☐	☐	☐

2. ¿Tiene usted buenos conocimientos de los estándares de seguridad de información?

Totalmente en Desacuerdo	*En Desacuerdo*	*Indeciso*	*De Acuerdo*	*Totalmente De Acuerdo*
☐	☐	☐	☐	☐

3. ¿Conoce usted bien el documento de clasificaciones establecidas para la seguridad de la información en la Universidad ?

Totalmente en Desacuerdo	*En Desacuerdo*	*Indeciso*	*De Acuerdo*	*Totalmente De Acuerdo*
☐	☐	☐	☐	☐

4. ¿Usted tiene claramente definida y establecida la propiedad de la información de acuerdo a lo asignado por la Universidad?

Totalmente en Desacuerdo	*En Desacuerdo*	*Indeciso*	*De Acuerdo*	*Totalmente De Acuerdo*
☐	☐	☐	☐	☐

5. ¿Sabe con exactitud sobre los programas para sensibilización de seguridad de la información a dictar a todos los empleados?

Totalmente en Desacuerdo	***En Desacuerdo***	***Indeciso***	***De Acuerdo***	***Totalmente De Acuerdo***
☐	☐	☐	☐	☐

6¿Tiene claras las políticas de seguridad de la información de la institución?

Totalmente en Desacuerdo	***En Desacuerdo***	***Indeciso***	***De Acuerdo***	***Totalmente De Acuerdo***
☐	☐	☐	☐	☐

7. ¿Tiene claro el plan de continuidad de operaciones de la institución?

Totalmente en Desacuerdo	***En Desacuerdo***	***Indeciso***	***De Acuerdo***	***Totalmente De Acuerdo***
☐	☐	☐	☐	☐

8. ¿En su institución tienen plan eficiente de recuperación ante desastres ?

Totalmente en Desacuerdo	***En Desacuerdo***	***Indeciso***	***De Acuerdo***	***Totalmente De Acuerdo***
☐	☐	☐	☐	☐

9.¿Considera usted que en la institución se han realizado con éxito una evaluación de riesgos de la información?

Totalmente en Desacuerdo	***En Desacuerdo***	***Indeciso***	***De Acuerdo***	***Totalmente De Acuerdo***
☐	☐	☐	☐	☐

10. ¿Considera que el riesgo de virus en la institución es alto?

Totalmente en Desacuerdo	***En Desacuerdo***	***Indeciso***	***De Acuerdo***	***Totalmente De Acuerdo***
☐	☐	☐	☐	☐

Anexo "E" Validación de Instrumentos de Recolección de Datos

Señor(a):

_____

Ciudad.

Ref. Validación de Instrumentos de Recolección de Datos

Por medio de la presente, me dirijo a Usted, como experto en el área, para informarle, que ha sido seleccionado (a) para la validación de los instrumentos a utilizar en el desarrollo de la investigación, la cual se titula: **"DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD NACIONAL EXPERIMENTAL POLITECNICA "ANTONIO JOSE DE SUCRE" SEDE RECTORAL"**

A tal fin, se anexa cuadro de operacionalización de variables, los instrumentos de recolección de datos (Entrevista y Cuestionario) 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,

_____

Lcdo. Manuel Mujica

Objetivos de la Investigación

Objetivo General

Diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

Objetivos Específicos

- Diagnosticar la situación actual en la que se encuentra la seguridad informática en la Universidad Nacional Experimental Politécnica "Antonio José de Sucre". sede Rectoral.
- Determinar la factibilidad operativa, técnica y económica de diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.
- Diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.
- Evaluar el Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral.

Operacionalización de las Variables

Variable en Estudio	Dimensión	Indicadores	Instrumentos	Fuente
"Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral"	Seguridad de información	○ 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 Acceso. ○ Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. ○ Gestión de Incidentes de Seguridad de la Información. ○ Gestión de la Continuidad Comercial. ○ Conformidad.	○ Entrevistas ○ Cuestionario ○ Observación Directa.	○ Coordinaciones ○ Personal OCTSI

Nota: Autor (2.006)

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO
Maestría en Ciencias de la Computación

Formato para la Revisión y Validación del Instrumento de Recolección de Datos

Apellidos y Nombre: _____
Título que posee: _____
Especialidad de Postgrado: _____
Cargo que Desempeña: _____

INSTRUCCIONES

- Lea detenidamente cada uno de los ítemes 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.

Formato de validación del Instrumento (Entrevista)

Ítem	Pregunta	Claridad		Congruencia		Redacción		Observaciones
		Si	No	Si	No	Si	No	
1	¿Indique si la Universidad esta certificada en alguno de los estándares de seguridad de información e indicar de ser afirmativo el estándar, fecha de certificación y entidad certificadora?							
2	¿Conoce usted alguno de los estándares de seguridad de información y de ser afirmativo mencione como adquirió usted este conocimiento?							
3	¿Indique las clasificaciones de seguridad de información actualmente existentes en la Universidad?							
4	¿Indique el uso que se le da a la información según las clasificaciones existentes en la institución?							
5	¿Indique si la institución posee programas dirigidos a sensibilizar sobre la seguridad de la información para todos los empleados?							
6	¿Las políticas de seguridad son para toda la institución o solo para la dirección de tecnología?							
7	¿Existe un documento que reúne todas las políticas de seguridad de información vigentes?							
8	¿Existe un procedimiento para actualizar periódicamente el documento de políticas de seguridad?							

Ítem	Pregunta	Claridad		Congruencia		Redacción		Observaciones
		Si	No	Si	No	Si	No	
9	¿Existe un archivo de Seguridad de Información que reúne todos los convenios vigentes en este sentido?							
10	¿En su institución el plan de continuidad de operaciones cuando se definió o actualizó por última vez, indique si hizo algún simulacro en los últimos seis meses y cuales recomendaron en dicha oportunidad acciones urgentes a realizar para reducir riesgos?							
11	¿En la institución indique cual es el plan de recuperación ante desastres que se tiene y si hizo algún simulacro en los últimos seis meses e indique cuales recomendaciones se realizaron en dicha oportunidad para reducir el riesgos?							
12	¿En la institución han realizado en alguna oportunidad una evaluación de riesgos de la información?							
13	¿En la institución han realizado una evaluación de vulnerabilidades de la red y de ser afirmativo ha sido en los últimos seis meses?.							
14	¿En la institución han realizado pruebas de penetración perimetral y de ser afirmativo se recomendaron en dicha oportunidad acciones urgentes a realizar para reducir riesgos?							
15	¿En su institución tienen software antivirus y de ser afirmativo indique la fecha de su última actualización.?							
16	¿En su institución tienen software para detección de intrusos?							

Fecha: _____ Firma: _____

Formato de validación del Instrumento (Cuestionario)

Ítem	Pregunta	Claridad		Congruencia		Redacción		Observaciones
		Si	No	Si	No	Si	No	
1	¿Considera usted que la Universidad tiene certificación en alguno de los estándares de seguridad de información?							
2	¿Tiene usted buenos conocimientos de los estándares de seguridad de información?							
3	¿Conoce usted bien el documento de clasificaciones establecidas para la seguridad de la información en la Universidad ?							
4	¿Usted tiene claramente definida y establecida la propiedad de la información de acuerdo a lo asignado por la Universidad?							
5	¿Sabe con exactitud sobre los programas para sensibilización de seguridad de la información a dictar a todos los empleados?							
6	¿Tiene claras las políticas de seguridad de la información de la institución?							
7	¿Tiene claro el plan de continuidad de operaciones de la institución?							
8	¿En su institución tienen plan eficiente de recuperación ante desastres ?							
9	¿Considera usted que en la institución se han realizado con éxito una evaluación de riesgos de la información?							
10 2.	¿Considera que el riesgo de virus en la institución es alto?							

Nota: Para dar respuestas al Cuestionario se utiliza una escala Likert según se muestra a continuación:

Totalmente en Desacuerdo	***En Desacuerdo***	***Indeciso***	***De Acuerdo***	***Totalmente De Acuerdo***
☐	☐	☐	☐	☐

Fecha: _____ ***Firma:*** _____

Anexo "F" Confiabilidad del Instrumento

Resumen del procesamiento de los casos

	Casos					
	Incluidos		Excluidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
P.1	5	100,0%	0	,0%	5	100,0%
P.2	5	100,0%	0	,0%	5	100,0%
P.3	5	100,0%	0	,0%	5	100,0%
P.4	5	100,0%	0	,0%	5	100,0%
P.5	5	100,0%	0	,0%	5	100,0%
P.6	5	100,0%	0	,0%	5	100,0%
P.7	5	100,0%	0	,0%	5	100,0%
P.8	5	100,0%	0	,0%	5	100,0%
P.9	5	100,0%	0	,0%	5	100,0%
P.10	5	100,0%	0	,0%	5	100,0%

Resúmenes de casos

	P.1	P.2	P.3	P.4	P.5	P.6	P.7	P.8	P.9	P.10
1	1	2	1	1	1	2	2	2	1	4
2	1	1	1	1	1	1	2	1	1	4
3	1	2	1	1	1	1	1	1	1	5
4	1	2	1	1	1	1	1	1	1	5
5	2	2	2	2	2	2	2	2	3	4
Total N	5	5	5	5	5	5	5	5	5	5

Análisis de fiabilidad (Alpha)

```
 ****** Method 1 (space saver) will be used for this analysis ******


  R E L I A B I L I T Y  A N A L Y S I S  -  S C A L E  (A L P H
A)


Reliability Coefficients

N of Cases =      5,0                    N of ítems = 10

Alpha =    ,8586
```

Anexo “G” Resúmenes de Casos

Resúmenes de casos

Casos	P.1	P.2	P.3	P.4	P.5	P.6	P.7	P.8	P.9	P.10
1	3	2	2	2	2	2	2	3	3	5
2	2	2	2	5	2	4	4	4	2	4
3	2	4	3	2	2	1	1	1	1	3
4	1	2	1	2	1	2	1	2	2	1
5	2	2	2	2	2	1	4	2	2	4
6	2	4	2	4	1	2	3	4	3	2
7	2	4	2	2	2	2	3	2	3	2
8	1	4	4	3	2	4	2	2	3	4
9	1	2	2	4	2	2	2	2	3	2
10	3	4	3	4	4	3	4	3	2	2
11	1	1	1	2	1	2	1	1	1	1
12	2	2	1	2	2	3	1	2	2	3
13	4	4	2	3	2	4	5	3	2	5
14	2	2	4	4	2	4	3	2	2	2
15	1	2	1	1	1	1	1	1	1	2
16	1	2	1	1	1	2	2	2	1	4
17	1	1	1	1	1	1	2	1	1	4
18	1	2	1	1	1	1	1	1	1	5
19	1	2	1	1	1	1	1	1	1	5
20	2	2	2	2	2	2	2	2	3	4
Total N	20	20	20	20	20	20	20	20	20	20

Anexo "H" Tabla de frecuencia

P.1 ¿Considera usted que la Universidad tiene certificación en alguno de los estándares de seguridad de información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	9	45,0	45,0	45,0
	2	8	40,0	40,0	85,0
	3	2	10,0	10,0	95,0
	4	1	5,0	5,0	100,0
	Total	20	100,0	100,0	

P.2 ¿Tiene usted buenos conocimientos de los estándares de seguridad de información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	2	10,0	10,0	10,0
	2	12	60,0	60,0	70,0
	4	6	30,0	30,0	100,0
	Total	20	100,0	100,0	

P.3 ¿Conoce usted bien el documento de clasificaciones establecidas para la seguridad de la información en la Universidad ?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	8	40,0	40,0	40,0
	2	8	40,0	40,0	80,0
	3	2	10,0	10,0	90,0
	4	2	10,0	10,0	100,0
	Total	20	100,0	100,0	

P.4 ¿Usted tiene claramente definida y establecida la propiedad de la información de acuerdo a lo asignado por la Universidad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	5	25,0	25,0	25,0
	2	8	40,0	40,0	65,0
	3	2	10,0	10,0	75,0
	4	4	20,0	20,0	95,0
	5	1	5,0	5,0	100,0
	Total	20	100,0	100,0	

P.5 ¿Sabe con exactitud sobre los programas para sensibilización de seguridad de la información a dictar a todos los empleados?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	8	40,0	40,0	40,0
	2	11	55,0	55,0	95,0
	4	1	5,0	5,0	100,0
	Total	20	100,0	100,0	

P.6 ¿Tiene claras las políticas de seguridad de la información de la institución?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	6	30,0	30,0	30,0
	2	8	40,0	40,0	70,0
	3	2	10,0	10,0	80,0
	4	4	20,0	20,0	100,0
	Total	20	100,0	100,0	

P.7 ¿Tiene claro el plan de continuidad de operaciones de la institución?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	7	35,0	35,0	35,0
	2	6	30,0	30,0	65,0
	3	3	15,0	15,0	80,0
	4	3	15,0	15,0	95,0
	5	1	5,0	5,0	100,0
	Total	20	100,0	100,0	

P.8 ¿En su institución tienen plan eficiente de recuperación ante desastres ?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	6	30,0	30,0	30,0
	2	9	45,0	45,0	75,0
	3	3	15,0	15,0	90,0
	4	2	10,0	10,0	100,0
	Total	20	100,0	100,0	

P.9 ¿Considera usted que en la institución se han realizado con éxito una evaluación de riesgos de la información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	7	35,0	35,0	35,0
	2	7	35,0	35,0	70,0
	3	6	30,0	30,0	100,0
	Total	20	100,0	100,0	

P.10 ¿Considera que el riesgo de virus en la institución es alto?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	2	10,0	10,0	10,0
	2	6	30,0	30,0	40,0
	3	2	10,0	10,0	50,0
	4	6	30,0	30,0	80,0
	5	4	20,0	20,0	100,0
	Total	20	100,0	100,0	

Anexo "I". Documentación de seguridad existente.

Requerimientos de seguridad para el ambiente de TI

- Usuarios y/o Estaciones de trabajo
  - Ambiente restrictivo con solamente acceso a los servicios básicos
  - Acceso a puertos USB y seriales bloqueados
  - Acceso a Unidades de Floppy Disk bloqueados
  - Acceso a unidades de CD solo lectura
  - Acceso al disco duro limitado (No podrán borrar archivos)
  - Acceso a puertos Wireless bloqueado
  - Monitoreo remoto de usuarios activos por administrador
  - Mensaje de login indicando restricciones y que sus actividades están siendo monitoreadas.
  - Sistema de archivo en servidor que pueda ser visto por el usuario y los que se definan que pueden tener acceso.
  - Acceso al panel de control restringido
  - Logs de seguridad activados
  - Software de registro de actividad activado (Keylogger)
  - Uso de los equipos en horario de 7:00 AM a 7:00 PM, en caso de requerir más tiempo debe ser expresamente autorizado.
  - Cuenta Guest deshabilitada
  - Solamente activo el protocolo TCP/IP
  - Mantener antivirus actualizado
  - Mantener el último service pack instalado
  - No permitir Chat
  - No permitir bajar música
  - No permitir acceso a Hotmail
  - Misceláneos

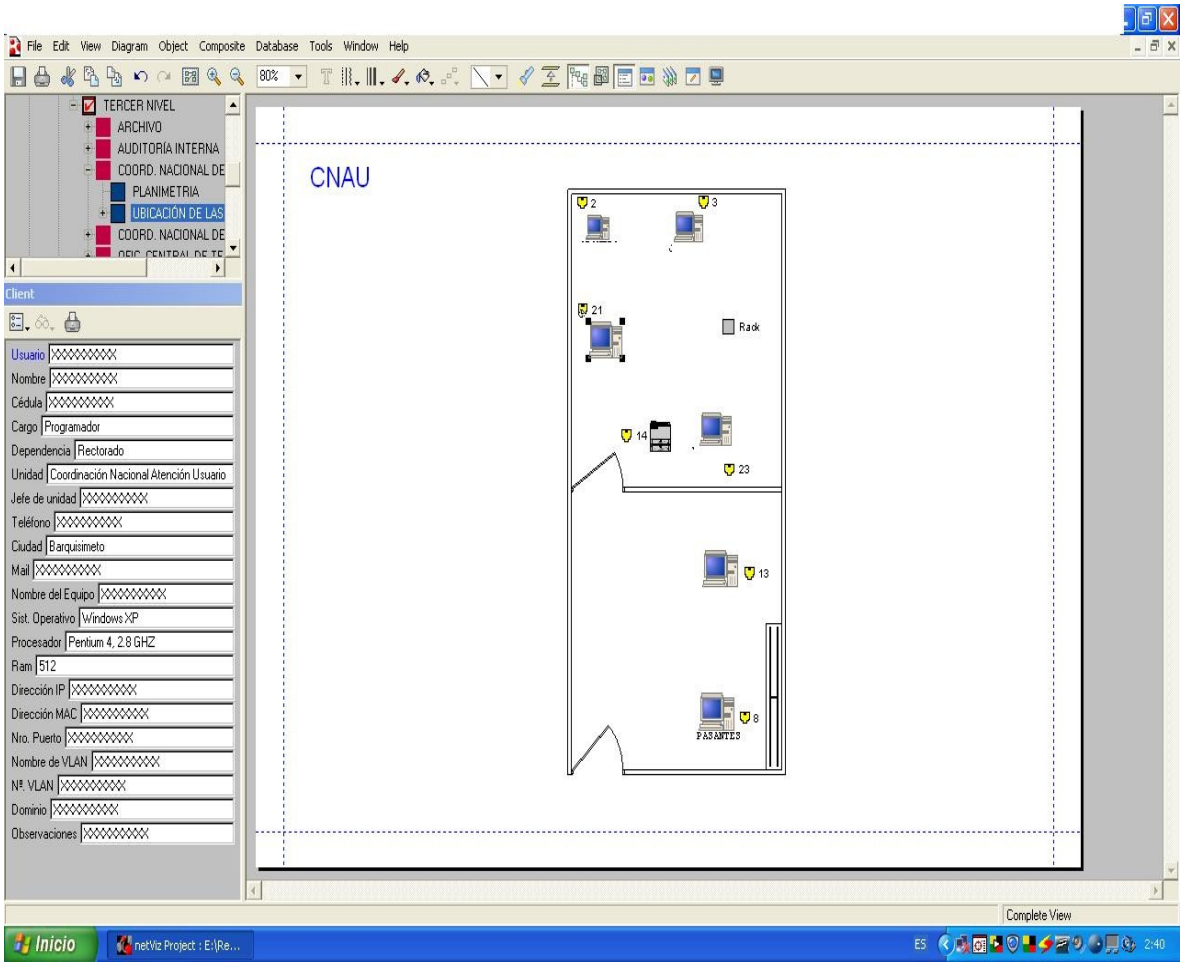
- Servidor
  - Solamente tiene acceso el administrador
  - Auditorías y archivos de Log activos
  - Backups programados en forma periódica con garantía funcional a tres (3) niveles
  - Solamente activo el protocolo TCP/IP
  - Deshabilitar la cuenta Guest
  - Mantener registro de logs y fallas de seguridad
  - Aplicar seguridad al menos C2
  - Mantener registros de accesos remotos
  - Mantener el último service pack, hotfixes y patches
  - Deshabilitar acceso anónimo
  - Deshabilitar NetBios sobre TCP/IP
  - Renombrar cuenta de administrador
  - Acceso remoto controlado y registrado
  - Implantar IPSec
  - Habilitar los siguientes registros de eventos
    - Logon y logoff, falla y existo
    - Acceso a archivos y objetos, fallas
    - Uso de derechos de usuarios, fallas
    - Administración de usuario y grupos, éxito y falla

        - Cambios en políticas de seguridad, éxito y fallas
        - Reinicio, apagado y sistema, éxito y fallas
    - Deshabilitar los servicios no autorizados
    - Misceláneos

- Servicios Básicos
    - Servicio de archivos
    - Servicio de Impresión
    - Servicio de navegación en Internet
    - Registro y autenticación con al menos dos (2) elementos
    - Servicio de correo electrónico
    - Servicio de FAX

Anexo “J”. Inventario de Hardware.

Se utilizó como herramienta el software NetViz, se muestra un ejemplo cuidando la confidencialidad de la información a continuación:



Anexo “K”. Inventario de Servicios.

Ejemplos

Formato Servidores

DATOS DE LOS SERVIDORES		SERVIDOR 1
Hardware		
Marca		HP
Modelo		ProLiant ML350 G4
Número de Serie		VSM51204RE
Etiqueta de Bienes Nacionales		
Tipo de Procesador		XEON
Cantidad de Procesadores		2
Marca del Procesador		Intel
Modelo del Procesador		XEON
Velocidad del Procesador		3.2 GHz
Capacidad total de Memoria Viva o RAM		2 GBytes
Capacidad total de Memoria en Discos		135,66 GBytes
Capacidad no usada de Memoria en Discos		
Cantidad de Discos		2
Software		
Sistema Operativo	Nombre y Versión	Windows 2003 Server
	Service Pack	SP 1 - 59 Fix de Seguridad
	Fix de Seguridad	Ultimo FIX: Actualización de seguridad para Windows Server 2003 (KB918439)-06/11/2006
Función principal del servidor		Servidor de Dominio
Funciones secundarias del servidor		DHCP/DNS/WINS
Servidores Lógicos		
Servicios Levantados		DC/DHCP/DNS/WINS
Dirección IP publicada		172.18.2.2 / 23
Otras Direcciones IP		
Aplicaciones		
Varios		
Producción / Desarrollo		Producción
Estatus		OK
Ubicación Física		CCPS
Observaciones		
Cambios		Actualización de FIX de seguridad

Formato equipo de comunicación.

DATOS DE EQUIPOS DE COMUNICACIÓN	EQUIPO1
Tipo / Función	Router
Marca	CISCO
Modelo	2501
Número de Serie	250094967
Etiqueta de Bienes Nacionales	
Interfaces / puertos	2 Seriales, 1 Ethernet
Sistema Operativo	IOS 11.2 (19a)
Ubicación Física	CCPS
Observaciones	

Formato de Servicios de Información

Ejemplo

Información sobre Custodio Técnico			
Nombre custodio	código único	ext	Ubicación
NA	NA	NA	NA

Descripción de La aplicación	Estatus	Mantenido por
como llevar el control de prestamos , reservaciones y de usuarios habituales de la biblioteca de igual modo llevar un control estadistico del uso de la biblioteca (EL MODULO DE ESTADISTICAS NO FUE IMPLEMENTADO)	Produccion	PO

Desarrollado por	Soporte Técnico	Frecuencia de Mantenimiento	Fuente	Ubicación de código fuente	Plataforma de Desarrollo
José Mujica		Ocasional	SI	Investigación y Postgrado	Stand alone

Lenguaje de programación	Idioma	Versión	Cantidad de licencias	Tipo de Licencias	Documentación Modelo de procesos	Actualizaciones
Clipper	Ingles	5	0		NO	NO

Parches	Interfaces	tipo de interfaces	Método de transmisión de interfaces	Requisitos de Operación
No	SAB	Entrada-Salida	NA	CPU: 486. RAM : 32 MB, SO: DOS, Modificacion de Autoexec.bar y config.sys

Información de Servidor de la aplicación								
Alcance	Criticidad operativa	Servidores donde esta la aplicación	Mac	Ip del servidor	Ubicación del Servidor(es)	Sistema operativo	Versión SO	Tipo de servidor
Local	SI	gerardo			Dirección de Investigación y Postgrado - Biblioteca	Windows XP	2002 SERVICE PACK 2	Aplicación

Información Básica de la Base de datos								
Nombre de Base de Datos	Manejador de Datos (DBMS)	Listerne	Versión de Base de Datos	Ambiente(s) de BD	Código embebido Trigger BD	Código embebido Function BD	Código embebido Package BD	Documentación Diccionario de datos
NA	NA	NA	NA	NA	NA	NA	NA	NO

Información de Servidor de la Base de Datos				
Servidor(es) de BD	Ip de servidor de BD	Ubicación de Servidor(es) de BD	Sistema O. Del Servidor de BD.	Versión de Sistema O. Del Servidor de BD
NA	NA	NA	NA	NA

Información Básica del Usuario		
Región	Dirección o Departamento	Cant. Usuario
V.R. Barquisimeto	Investigacion y Postgrado	3

Anexo “L”. Memoria fotográfica.

Curso dictado en UNEXPO en las aulas de Postgrado Barquisimeto en referencia a la implementación del las políticas en el área de Tecnología y elementos de Seguridad (mayo-julio 2005)

Anexo “M”. Perfiles usuarios.

Descripción de Directivas de Grupo Aplicadas

Es necesario indicar ahora algunos detalles respecto a la configuración de las directivas de grupo aplicadas en el dominio UNEXPO, como expresión de las políticas de seguridad generales implementadas por la Oficina Central de Tecnología y Servicios de Información para resguardar la seguridad de acceso a la red y las estaciones de trabajo de la Institución.

Directivas de usuario y de equipo

La configuración de la directiva de usuario está ubicada en Configuración de usuario en la Directiva de grupo y se obtiene cuando el usuario inicia una sesión. La configuración de la directiva de equipo está ubicada en Configuración de equipo y se obtiene al iniciar el equipo.

Los usuarios y los equipos son los únicos tipos de objetos de Active Directory que reciben directivas. Específicamente, la directiva no se aplica a los grupos de seguridad. En su lugar, por motivos de rendimiento, se utilizan grupos de seguridad para filtrar la directiva mediante una entrada de control de acceso (ACE) de Aplicar directiva de grupos, que se puede establecer en Permitir o en Denegar, o se puede dejar sin configurar.

Orden de aplicación

Las directivas se aplican en el orden siguiente:

- El objeto de directiva de grupo local único.
- Objetos de directiva de grupo del sitio, en el orden especificado por el administrador.
- Objetos de directiva de grupo del dominio, en el orden especificado por el administrador.
- Objetos de directiva de grupo de la unidad organizativa, de unidad organizativa mayor a menor (de principal a secundaria), en el orden especificado por el administrador en el nivel de cada unidad organizativa.

De forma predeterminada, las directivas aplicadas posteriormente sobrescriben las directivas aplicadas con anterioridad cuando son incoherentes. Sin embargo, si no hay incoherencias en las directivas, tanto las anteriores como las posteriores contribuyen a la eficacia de las directivas.

Filtrar la directiva en función de la pertenencia a grupos de seguridad

Una entrada ACE para un grupo de seguridad en un objeto de directiva de grupo puede establecerse como No configurada (no hay preferencia), Permitida o Denegada. Denegada tiene prioridad sobre Permitida.

Bloquear la herencia de directivas

Las directivas que normalmente se heredarían de sitios, dominios o unidades organizativas superiores se pueden bloquear en el nivel de sitio, dominio o unidad organizativa.

Aplicar la directiva desde arriba

Puede configurar directivas que de otro modo serían sobrescritas por directivas de unidades organizativas secundarias como No omitir en el nivel de objeto de directiva de grupo.

Las directivas que se han configurado como No omitir no se pueden bloquear. Las opciones No omitir y Bloquear deben utilizarse con moderación. El uso incontrolado de estas características avanzadas complica la solución de problemas.

Perfil Común

El perfil común, como su nombre lo indica, contiene todas las configuraciones que son comunes a todos los usuarios de la red institucional de datos de la UNEXPO.

Esta directiva es la única que presenta configuraciones de equipo: se establecen las configuraciones de seguridad y las plantillas administrativas. Entre los elementos que se establecen en este ámbito están las políticas de administración y control de contraseñas, el bloqueo del instalador de Windows para los usuarios del dominio, el direccionamiento de actualizaciones de Windows a un servidor local, entre otros.

En la configuración de usuario es, en realidad, donde se detallan las partes más importantes de las políticas de acceso aplicadas. Como primer elemento vale la pena mencionar que en la configuración de Windows se establecen los elementos de mantenimiento del Internet Explorer, tales como página de inicio, dirección de servidor Proxy y la lista de favoritos comunes.

En las plantillas administrativas de usuario están el grueso de las configuraciones. Este contenedor engloba los componentes de Windows, el menú de inicio y la barra de tareas, escritorio, panel de control, carpetas compartidas, red y sistemas. Se configura entonces el escritorio de acceso plano, con el menú de inicio casi vacío (a excepción de la configuración de impresoras) y el área de notificación de la barra de tareas únicamente con el reloj activo. Se bloquea el acceso al panel de control y el cambio de cualquier configuración de red.

Pero es en el contenedor de Sistema donde se hacen la mayor parte de las configuraciones comunes, como el bloqueo de varias aplicaciones (Messenger y Windows Media), el editor del registro, el administrador de tareas y la mayor parte de las carpetas del perfil móvil. Adicionalmente, se establece la ejecución de comandos comunes de inicio, actualmente configurado para mostrar una presentación por diapositivas con contenido informativo.

Perfil Básico

El perfil básico contiene la configuración de Windows para los usuarios comunes de la red. No presenta nuevas configuraciones de equipo respecto del perfil común, sino especificidades en la configuración de usuarios, tales como el bloqueo del acceso a discos (A, B y C) y el bloqueo de ejecución de línea de comandos.

Perfil Directivo

Se trata del mismo perfil básico, con la adición del acceso a Internet realizado en el servidor Proxy por el administrador de este servicio.

Perfil Desarrollo Web

Este perfil, al igual que el básico, sólo presenta configuraciones de usuario. Las más importantes son el acceso al área de notificación de la barra de tareas y la restricción de discos reducida sólo a las unidades A y B.

Perfil Acceso a Unidades (Temporal)

Este perfil, creado para solventar una necesidad temporal, podría resolver las necesidades de la mayor parte de los directivos de la institución, que necesitan mayor portabilidad de información. Tiene como peculiaridad el acceso a todas las unidades de disco (excepto el disco de sistema, C) y al área de notificación de la barra de tareas.

Perfil Acceso a Disquete (Temporal)

Este perfil, permite el acceso a la unidad de disquetes, para permitir el uso de una cámara digital que no posee otro medio de transmisión para las imágenes.

Descripción de los Perfiles Móviles

En los equipos con sistemas operativos Windows Server 2003, los perfiles de usuario crean y mantienen automáticamente la configuración de escritorio del entorno de trabajo de cada usuario en el equipo local. El perfil de usuario se crea cuando el usuario inicia por primera vez una sesión en el equipo.

El uso de los perfiles de usuario ofrece varias ventajas:

- Varios usuarios pueden utilizar el mismo equipo. Cuando los usuarios inician una sesión en sus estaciones de trabajo, reciben la configuración de escritorio que tenían al terminar la última sesión.
- La personalización del entorno de escritorio efectuada por un usuario no afecta a la configuración del resto de los usuarios.
- Los perfiles de usuario se pueden almacenar en un servidor para que los usuarios puedan utilizarlos en cualquier equipo de la red que ejecute Microsoft Windows NT o posterior. Este tipo de perfiles se denominan perfiles de usuario móvil.

Como herramienta administrativa, los perfiles de usuario ofrecen estas opciones:

- Puede crear un perfil de usuario predeterminado que sea adecuado a las tareas del usuario.
- Puede configurar un perfil de usuario obligatorio que no guarde las modificaciones del escritorio que haya efectuado el usuario. Los usuarios pueden modificar la configuración del escritorio en el equipo durante la sesión, pero no se guarda ningún cambio cuando la terminan. La configuración del perfil obligatorio se descarga en el equipo local siempre que el usuario inicia la sesión. Para obtener información acerca de los perfiles obligatorios, consulte Para crear un perfil de usuario obligatorio.
- Puede especificar la configuración de usuario predeterminada y que quede incluida en todos los perfiles de usuario individuales.

Tipos de perfiles de usuario

Los perfiles de usuario definen entornos de escritorio personalizados, en los que se incluye la configuración individual de la pantalla, las conexiones de red y de impresoras, y otras configuraciones especificadas. El usuario o el administrador del sistema pueden definir el entorno de escritorio.

Entre los tipos de perfiles de usuario se encuentran:

- *Perfil de usuario local*: el perfil de usuario local se crea la primera vez que un usuario inicia una sesión en un equipo y está almacenado en el disco duro local del equipo. Todas las modificaciones efectuadas en un perfil de usuario local son específicas del equipo concreto en el que se hayan realizado.
- *Perfil de usuario móvil*: los perfiles de usuario móviles los crea el administrador del sistema y se almacenan en un servidor. Este perfil está disponible siempre que el usuario inicia una sesión en cualquier equipo de la red. Los cambios efectuados en un perfil de usuario móvil se guardan en el servidor.

- *Perfil de usuario obligatorio*: los perfiles de usuario obligatorios son perfiles móviles que se utilizan para especificar configuraciones particulares de usuarios o grupos de usuarios. Sólo los administradores del sistema pueden realizar cambios en los perfiles de usuario obligatorios.
- *Perfil de usuario temporal*: el perfil de usuario temporal se emite siempre que una condición de error impide la carga del perfil del usuario. Este tipo de perfil se elimina al final de cada sesión. Los cambios realizados por el usuario en la configuración del escritorio y los archivos se pierden cuando cierra la sesión.

En la red institucional de datos de la UNEXPO están aplicados los perfiles móviles, que permiten a los usuarios virtualmente "llevar" su escritorio a cualquier estación de trabajo donde inicien sesión.

Los perfiles móviles están almacenados en el servidor de dominio, lo que hace necesario incluir una ruta DNS al mismo si la configuración de red se establece manualmente.

Almacenamiento de la Información

El servidor de dominio (actualmente "Reservado") sólo almacena los archivos de configuración de los perfiles móviles, los scripts de inicio de sesión y una carpeta compartida donde se almacenan las presentaciones de diapositivas de carácter informativo que publica periódicamente el Grupo de Trabajo Adiestramiento, tales como las noticias y el instructivo de uso de la red.

En el servidor de archivos (actualmente "Reservado") están las carpetas de información institucional de los usuarios, de acceso exclusivo para los mismos, sujetas a las políticas de respaldo establecidas por la Oficina Central de Tecnología y Servicios de Información. Adicionalmente, existe una carpeta compartida para cada unidad organizativa y a la cual solo acceden los miembros de la misma. Ambas carpetas de red se conectan a unidades de red prefijadas (Z para la personal y Y para la compartida), fácilmente asequibles por accesos directos previamente creados en el disco de datos de cada estación de trabajo, bajo los nombres de Institucional y Compartidos.

Recientemente, fue creada una carpeta compartida con acceso libre para todos los usuarios del Rectorado (llamada "Pública").

Anexo “N”. Herramientas de Rastreo, evaluación y ruptura de contraseñas.

A continuación se incluye una breve descripción de las herramientas utilizadas a lo largo de la evaluación de seguridad.

Advance Lan Scanner
Es una herramienta de utilidad para realizar funciones a través de una red de área local (LAN). Te permite obtener diversa información sobre los PC conectados a la red local en varios segundos, pero quizás los aspectos más interesantes son la posibilidad de apagado y encendido remoto y la integración total. Versión bajo windows

ADMsnmp
Utilidad unix de linea de comandos muy eficaz para forzar cadenas de comunidad SNMP.

Angry IP Scanner
Escaner de red para comprobar rápidamente que equipos se encuentran encendidos, versión bajo windows

bf_ldap
Herramienta unix para realizar ataques de fuerza bruta LDAP.

Brutus
Un cracker de autenticación de fuerza bruta para redes. Este cracker sólo para Windows se lanza sobre servicios de red de sistemas remotos tratando de averiguar passwords utilizando un diccionario y permutaciones de éste. Soporta HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, y más.

codeflux
Herramienta online de validación de sitios web y obtención de información.

doctorDNS
Es un sistema de diagnóstico del funcionamiento de los servidores de nombre para un cierto nombre de dominio. Su uso e interpretación está orientada hacia gente del área técnica, que conozca los detalles de operación de un DNS. desarrollado por NIC Chile.

enum
Es una herramienta de comando en línea para windows que realiza una gran cantidad de consultas al servidor objetivo ejecutando NetBIOS a través del puerto TCP 139. La herramienta puede realizar un listado de nombres de usuarios, políticas de contraseñas, elementos compartidos, etc.

Fping
Un programa para el escaneo con ping en paralelo.

Foundstone SuperScan
Utilidad de rastreo ICMP, TCP y UDP de redes basadas en la interfaz gráfica tradicional que utiliza el sistema Windows.

Free Port Scanner
Es una herramienta pequeña, rápida y robusta para el monitoreo de puertos. El programa utiliza paquetes TCP para determinar los puertos disponibles, servicios asociados a puertos y otras características importantes, versión bajo windows

ghba
La utilidad realiza barridos de DNS inversos de espacios de direcciones Clase B y C.

host y dig
Comandos de la plataforma Linux, esta utilidad realiza todo tipo de consulta DNS, incluyendo transferencia de zonas y consultas inversas.

Hping2
Una utilidad de observación para redes similar a ping. Hping2 ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado. También tiene un modo traceroute bastante útil y soporta fragmentación de IP.

N-Auditor
Es una herramienta multiusos diseñada para explorar redes y los anfitriones para las vulnerabilidades, y para proporcionar alarmas de la seguridad. Versión bajo windows

NetScantools
Es un programa que agrega utilidades de redes UNIX pero en versión para Windows. El programa es una colección de utilidades para la red como: finger, ping, traceroute, whois, daytime, quote, Winsock info, servicios de socket, protocolos de socket, y un capturador de URLs.

netcraf
Herramienta online Antiphishing que proporciona información sobre el sistemas y los servicios.

Nessus
Es la herramienta de evaluación de seguridad "Open Source" de mayor renombre. Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas.

nikto
Un escáner de web de mayor amplitud. Nikto es un escáner de servidores de web que busca más de 2000 archivos/CGIs potencialmente peligrosos y problemas en más de 200 servidores. Utiliza la biblioteca LibWhisker pero generalmente es actualizado más frecuentemente que el propio Whisker.

nmap
Es una utilidad de línea de comandos, rastreador de puertos diseñado para explorar grandes redes y determinar qué equipos se encuentran activos y cuáles son los servicios TCP y UDP que ofrecen. Nmap acepta la mayoría de las técnicas de rastreo ICMP, TCP, UDP más populares, ofreciendo además una gran cantidad de características avanzadas, como la identificación de IP, exploración silenciosa, la identificación de protocolos de servicios y análisis de filtros de bajo nivel.

nslookup
Esta utilidad realiza todo tipo de consulta DNS, incluyendo transferencia de zonas y consultas inversas.

N-Stealth
Es un escáner de seguridad de servidores de web no-libre. Es generalmente, actualizado más frecuentemente que los escáneres de web libres tales como whisker y nikto. Soportan 20.000 vulnerabilidades y exploits.

Retina
Escáner para la evaluación de vulnerabilidades no-libre hecho por eEye. Al igual que Nessus y ISS Internet Scanner, la función de Retina es escanear todos los hosts en una red y reportar cualquier vulnerabilidad encontrada.

telnet
Servicio de gestión remoto en texto plano que proporciona acceso mediante línea de comandos a múltiples sistemas operativos.

scanudp
Es un simple programa escrito en C para plataforma gnu/linux para escanear puertos UDP en computadoras remotas.

Shadow Security Scanner
El programa es capaz de detectar vulnerabilidades en Unix, Linux, FreeBSD, OpenBSD, Solaris, y todas las versiones de Windows, incluyendo 2003. Este escáner detecta, además, fallos en Cisco y HP, realizado 2.000 auditorías para cada uno de ellos. Soporta protocolos como FTP, SSH, Telnet, SMTP, DNS, Finger, HTTP, POP3, IMAP, NetBIOS, NFS, NNTP, SNMP, y proxies Squid, LDAP, HTTPS, SSL, todo el TCP/IP y UDP, más servicios del registro de Windows.

SuperScan
El escáner de TCP para Windows de Foundstone. Un escáner de puertos de TCP, pinger y resolvedor de nombres {"hostname resolver"} basado en connect().

Visual Route
Obtiene información de traceroute/whois y la grafica sobre un mapa del mundo.

W3C
Servicio de validación libre que comprueba documentos del Web en formatos como el HTML y XHTML para saber si hay conformidad a las recomendaciones de W3C y a otros estándares. Valida el contenido de RSS/Atom o stylesheets del CSS y encuentra acoplamientos rotos.

Webferret
Es una herramienta para obtener de forma sencilla información en Internet. Su funcionamiento se basa en la realización de consultas sobre el término que se desea encontrar en los buscadores más conocidos. Los resultados van apareciendo en una lista donde se han eliminado las direcciones duplicadas. Versión bajo windows

Websnake
Herramienta que guarda en el disco duro los contenidos de las páginas previamente seleccionadas. Versión bajo windows

wget
Es una herramienta de Software Libre que permite la descarga de contenidos desde servidores web de una forma simple. Su nombre deriva de «World Wide Web» (w), y de «obtener» (get), esto quiere

decir: obtener desde WWW. Actualmente soporta descargas mediante los protocolos HTTP, HTTPS y FTP. Versión bajo gnu/linux

Wireshark
Es un analizador de protocolos de red para Unix y Windows, y es libre, antiguo ethereal. Permite examinar datos de una red activa o de un archivo de captura en algún disco. Tiene varias características poderosas, incluyendo un completo lenguaje para filtrar y la habilidad de mostrar el flujo reconstruído de una sesión de TCP.

Anexo "O". Comparación Cualitativa.

Otro escenario ejecutado en esta investigación fue el de verificar cualitativamente la situación en la que se encuentra la Universidad objeto de estudio en referencia a otras seis (6) Universidades Nacionales. La muestra tomada para el análisis fue de doce por ciento (12%) del total de cuarenta y nueve (49) Universidades registradas en la Oficina Central de Planificación del Sector Universitario (2.006) OPSU[24] , siendo el criterio para la muestra el tomado por Ary y otros (1.985) quienes establecen que "en las investigaciones descriptivas es recomendable seleccionar un diez (10) a veinte por ciento (20%) de la población accesible".

Las Universidades fueron seleccionadas de la siguiente manera: una (1) de manera intencional y cinco (5) al azar. Por ética profesional, no se coloca el nombre de las Universidades seleccionadas y en su lugar se le asignaron valores numéricos para resguardo de su identidad, lo que si se puede indicar es que cuatro (4) son de carácter públicas con infraestructura en todo el país, una (1) pública con infraestructura en la región centro occidental y una (1) privada con infraestructura en la región centro occidental.

La comparación entre universidades se estableció cualitativamente en función del escalamiento Líkert siendo sus valores: Excelente, Buena, Regular, Mala, Muy Mala, a continuación se muestran los resultados obtenidos:

[24] OPSU: Es un organismo que asesora y apoya a las instituciones de educación superior en la realización de sus funciones, así como en las normas y procedimientos para su funcionamiento y desarrollo de programas. http://www.cnu.gov.ve/informacion/opsu.php

a. Técnicas de Enumeración de servidores de Internet y de Redes.

Enumerar detalles de contactos Universidades

ítem	Universidad No. 1	Universidad No. 2	Universidad No. 3	Universidad No. 4	Universidad No. 5	Universidad No. 6	UNEXPO
Enumeración	716	36	89	8	36	56	14
Comparación	Muy Mala	Regular	Mala	Excelente	Regular	Mala	Buena

Nota: Autor (2007).

En el cuadro se muestra a la Unexpo en una posición "buena" en comparación cualitativa con respecto a las otras universidades.

Consulta Network Informations Centers (NIC) y DNS

NIC Universidades

ítem	Universidad No. 1	Universidad No. 2	Universidad No. 3	Universidad No. 4	Universidad No. 5	Universidad No. 6	UNEXPO
Creación	17/11/2005	17/11/2005	01/01/1998	01/01/1998	17/11/2005	11/12/2000	01/01/1998
Actualización	23/11/2005	17/11/2005	28/07/2006	17/11/2005	17/11/2005	31/03/2006	22/03/2006
Declarados	3	2	2	2	1	2	2
Funcionando	3	1	1	2	1	2	2
Comparación	Excelente	Mala	Mala	Buena	Regular	Buena	Buena

Nota: Autor (2007).

En el cuadro, se muestra a la Unexpo en una posición "buena" en comparación cualitativa con respecto a las otras universidades.

Tabla leyenda DNS

No.	Leyenda	Observación
0	Ok	En perfectas condiciones.
1	Con recursividad	Corresponde a un error grave. Un servidor autoritativo no debe ser recursivo, pues está sujeto a ataques de Cache Poisoning. Dicho ataque consiste en alterar la información entregada por el DNS mediante respuestas inválidas, pues un servidor recursivo averigua y memoriza las respuestas que recibe.
2	Error consultando vía TCP	El RFC 1035 indica que un servidor de DNS debe soportar consultas vía UDP y TCP. Aunque en general se prefiere UDP, TCP se utiliza para las transferencias de zona y para contestar consultas cuya respuesta excede los 512 bytes. (Mayores referencias en la sección 4.2 y 4.2.2 del RFC ya mencionado).
3	Servidor no Disponible	Es un error grave, porque implica que un servidor de nombres delegado no es alcanzable por diferentes razones: No resuelve número IP, no contesta válidamente, no es alcanzable a nivel de la red. Esto puede producir errores temporales de resolución.

Nota: Autor (2007).

DNS Universidades

DNS	Universidad No. 1			Universidad No. 2		Universidad No. 3		Universidad No. 4		Universidad No. 5	Universidad No. 6		UNEXPO	
	A	B	C	A	B	A	B	A	B	A	A	B	A	B
Serial Sync	Ok	Ok	Ok	Ok	3	3	Ok	Ok	Ok	Ok	Ok	Ok	Ok	Ok
Autoridad	Ok	Ok	Ok	Ok	3	3	Ok	Ok	Ok	Ok	Ok	Ok	Ok	Ok
Recursividad	Ok	Ok	1	Ok	3	3	1	Ok	Ok	1	Ok	Ok	1	1
Soporte TCP	Ok	Ok	2	Ok	3	3	Ok	2	2	Ok	2	2	Ok	Ok
Comparación	Bueno			Malo		Muy Malo		Bueno		Regular	Bueno		Bueno	

Nota: Autor (2007).

En el cuadro, se muestra a la Unexpo en una posición “buena” en comparación cualitativa con respecto a las otras universidades.

b. Exploración de redes IP

Exploración de redes IP Universidad

Servidores públicos DMZ	Universidad No. 1	Universidad No. 2	Universidad No. 3	Universidad No. 4	Universidad No. 5	Universidad No. 6	UNEXPO
Responde a Rastreo ICMP	No	No	Si	No	No	No	No
Abre puertos TCP necesarios	Si	Si	Si	Si	Si	Si	Si
Abre puertos UDP necesarios	Si	Si	Si	Si	Si	Si	Si
Comparación	Muy Buena	Muy Buena	Mala	Muy Buena	Muy Buena	Muy Buena	Muy Buena

Nota: Autor (2007).

En el cuadro cuarenta (40), se muestra a la Unexpo en una posición “muy buena” en comparación cualitativa con respecto a las otras universidades.

c. Evaluar servicios Web

Evaluar servicios Web Universidad

ítem	Universidad No. 1	Universidad No. 2	Universidad No. 3	Universidad No. 4	Universidad No. 5	Universidad No. 6	UNEXPO
Vulnerabilidades	220	17	15	12	2	5	7
Errores	111	99	25	33	31	30	19
Comparación	Muy Mala	Muy Mala	Mala	Mala	Regular	Regular	Buena

Nota: Autor (2007).

En el cuadro, se muestra a la Unexpo en una posición “buena” en comparación cualitativa con respecto a las otras universidades.

Anexo "P". Directrices para la auditoría

PROGRAMA DE AUDITORÍA

AREAS DE LA UNIVERSIDAD	FECHAS CALENDARIO		
	Día No. 1	Día No. 2	Día No. 3
Rectorado			
OCTSI			
Finanzas			

PLAN DE AUDITORÍA

Empresa a evaluar:	UNEXPO RECTORADO
Dirección de la Empresa a Evaluar	BARQUISIMETO
Objetivo de la Auditoría:	Auditar el sistema de gestión de seguridad
Alcance:	Las Operaciones de la Universidad, contemplando los procesos del: Rectorado, OCTSI y Finanzas
Auditoría	1
Grupo de Auditores:	3
Idioma(s) en que se desarrollará la auditoría	ESPAÑOL
Responsable por la Empresa de la Evaluación a realizar	COORDINADOR NACIONAL DE TECNOLOGIA DE INFORMACION

Lista de Chequeo Auditoría ISO 27001:2005

UNIVERSIDAD UNEXPO.		
EVIDENCIAS DE:	SI	NO
ALCANCE		
POLITICAS DE SEGURIDAD		
VALUACION DEL RIESGO		
IDENTIFICACIÓN DEL RIESGO		
ANALISIS DEL RIESGO		
TRATAMIENTO DEL RIESGO		
SELECCIÓN DE CONTROLES		
APROBACIÓN / AUTORIZACIÓN		
ENUNCIADO DE APLICATIVIDAD		

CRONOGRAMA DE AUDITORÍA ISO 27001:2005 CORRESPONDIENTE AL PLAN:

EMPRESA: UNEXPO RECTORADO
FECHA DE AUDITORÍA: Del___al___de_____
PROPÓSITO: " Verificar el Grado de conformidad del SGSI con respecto a la ISO 27001:2005
ALCANCE: "Las Operaciones la Universidad, contemplando los procesos de: Rectorado, OCTSI y Finanzas

NRO	ACTIVIDAD, PROCESO O REQUISITO (S)	REQUISITOS (S) ISO 27001:2005 DE LOS PROCESOS	RESPONSABLE DEL PROCESO O REQUISITO (S)	FECHA	HORA (INICIO Y FINAL)
1	Reunión de Apertura		RECTORA	1	9:00am - 9:30 am
2	Análisis de la Documentación, Revisión del Alcance, Política y Objetivo de Seguridad.	4.2.1	RECTORADO	1	9:30am - 10:30 am
3	Análisis y Evaluación del Riesgo: Identificación de Activos y Tasación	4.2.1	RECTORADO	1	10:30am - 11:30 am
4	Metodología para el Análisis y Evaluación del Riesgo	4.2.1	RECTORADO	1	11:30am - 12:30 pm
5	ALMUERZO			1	12:30 pm - 02:00 pm
6	Proceso de Selección de Controles	4.2.1	RECTORADO	1	02:00 pm - 03:00 pm
7	Revisión del Enunciado de Aplicabilidad	4.2.1	RECTORADO	1	03:00 pm - 04:00 pm
	Manejo del Proceso de Reportes de Incidentes	4.3	RECTORADO	1	04:00 pm - 05:00 pm

NRO	ACTIVIDAD, PROCESO O REQUISITO (S)	REQUISITOS (S) ISO 27001:2005 DE LOS PROCESOS	RESPONSABLE DEL PROCESO O REQUISITO (S)	FECHA	HORA (INICIO Y FINAL)
1	Cierre del día Anterior		RECTORA	2	9:00am - 9:30 am
2	Análisis y Evaluación del Riesgo: Identificación de Activos y Tasación	4.2.1	DIRECTOR OCTSI	2	09:30am - 11:30 am
3	Metodología para el Análisis y Evaluación del Riesgo	4.2.1	DIRECTOR OCTSI	2	11:30am - 12:30 pm
4	ALMUERZO			2	12:30 pm - 02:00 pm
5	Proceso de Selección de Controles	4.2.1	DIRECTOR OCTSI	2	02:00 pm - 03:00 pm
6	Revisión del Enunciado de Aplicabilidad	4.2.1	DIRECTOR OCTSI	2	03:00 pm - 04:00 pm
7	Manejo del Proceso de Reportes de Incidentes de Seguridad.	4.3	DIRECTOR OCTSI	2	04:00 pm - 05:00 pm

NRO	ACTIVIDAD, PROCESO O REQUISITO (S)	REQUISITOS (S) ISO 27001:2005 DE LOS PROCESOS	RESPONSABLE DEL PROCESO O REQUISITO (S)	FECHA	HORA (INICIO Y FINAL)
1	Cierre del día Anterior		RECTORA	3	9:00am - 9:30 am
2	Análisis y Evaluación del Riesgo: Identificación de Activos y Tasación	4.2.1	FINANZAS	3	09:30am - 10:30 am
3	Metodología para el Análisis y Evaluación del Riesgo	4.2.1	FINANZAS	3	10:30am - 11:30 pm
5	Proceso de Selección de Controles	4.2.1	FINANZAS	3	11:30 am - 12:30 pm
4	Revisión del	ALMUERZO		3	12:30 pm - 02:00 pm
6	Enunciado de Aplicabilidad	4.2.1	FINANZAS	3	02:00 pm - 2:30 pm
7	Manejo del Proceso de Reportes de Incidentes de Seguridad.	4.3	FINANZAS	3	02:30 pm - 03:00 pm
8	Preparación del Informe		AUDITOR	3	03:00 pm - 04:30 pm
9	Reunión Cierre		RECTORA	3	04:30 pm - 05:30 pm

LISTA DE CHEQUEO ESPECÍFICA
NOMBRE DEL AUDITADO: UNEXPO

PERSONAL

Pregunta	Métodos de revisión	NOTAS
Qué Significado tiene para usted la política de Seguridad de Información(SI) y que otras políticas conoce en materia de SI	La política le ha sido comunicada y tiene acceso a ella	
Cuáles son sus responsabilidades en materia de Seg.Info.	Verificar documento de roles y responsabilidades.	

METODOS

Pregunta	Métodos de revisión	NOTAS
Qué método utilizo para llegar al enunciado de aplicabilidad	Verificar existencia del documento	
Bajo que metodología determina la eficacia del tratamiento de controles	revisión del sistema e informes de auditorías anteriores, revisión por la dirección	

CONTROLES

Pregunta	Métodos de revisión	NOTAS
Qué criterios de aceptación y riesgos aceptables existen y para cuales?	registros de medición	
existe medición del riesgo residual	informe	

ACTIVOS

Pregunta	Métodos de revisión	NOTAS
Cómo fueron identificados los activos	revisión de reuniones de las partes interezadas	
amenazas y vulnerabilidades	informe	

Reporte de No Conformidad

Reporte de No Conformidad	Emisión / /	Documento No.
Generado por: Auditor	Revisado por:	Fecha de revisión:
No conformidad **Observación:** **Cláusula _____**		
Redacción de la No Conformidad u Observación _____ _____ _____ _____ _____ _____ _____ _____		
Evidencia objetiva _____ _____ _____ _____ _____ _____ _____ _____		

Anexo "Q". Implementaciones en seguridad UNEXPO

Equipos de comunicación

Router

Actualmente, mediante este equipo se restringen los accesos a los servidores públicos (Web, e-mail, DNS, etc) de la institución a través de las Listas de Control de Acceso (ACL) las cuales permiten el acceso a los puertos necesario para el uso de los servicios como por ejemplo: En el caso del servidor web que provee los servicios de acceso Web y DNS se permitirá el únicamente los puertos 80 y 53 respectivamente. Cabe destacar que esto se debe hacer en el Firewall (Hardware) del Campus.

Switch Capa 3(Principal)

Como es dispositivo posee capacidad de enrutamiento a nivel de Capa de red – IP, y los servidores internos (Antivirus, DHCP, Dominio, Archivo, Aplicaciones, etc) están ubicados en dicho equipo, se pueden permitir el acceso de todas la oficinas definidas en VLAN únicamente al servicio que este proveyendo dichos servidores.

Instalación de Switches (Secundarios)

Características Hardware:

- 24 de 10/100/1000 Mbps UTP Full-Duplex. (Módulos Hot-Swappable).
- 4 para módulos de Fibra Óptica Multimodo 1 Gbps Full/Duplex y sus respectivos módulos.
- Capacidad de Capa2 y Capa 3 con conmutación en Hardware.

Características Software:

- Fácil actualización de Firmware o Sistema Operativo.
- Capacidad VLAN con etiquetado de IEEE 802.1Q.
- Soporte del protocolo Spanning-Tree (STP-802.1D), Rapid Spanning-Tree (802.1w).
- Soporte para IPv4 e IPv6.
- DHCP Relay y UDP/TCP Relay (Active Directory).

Servidores

Servidor de Autenticación o Dominio (Active Directory)

A través de este Servidor (Active Directory) se aplican todas las políticas de acceso y uso de las estaciones de trabajo a todos los usuarios de la red como por ejemplo el tipo de acceso a Internet (Limitado, Intermedio e Ilimitado), el acceso o no de las unidades de diskette, USB, CD, etc…, uso de messeneger, kazaa, etc…., instalación de aplicaciones, modificación del sistema, etc.

Servidor de Antivirus

Se tiene instalado un software de Antivirus Corporativo, el cual se esta actualizado constantemente para que de está forma se actualicen todos los clientes de antivirus que deben estar instalados en todas las estaciones de trabajo y los servidores; En el caso de la UNEXPO se posee el software Symantec Corporate Edition.

Servidor de Actualizaciones de Seguridad (Windows Update)

El servicio de actualizaciones de seguridad (Windows Update) permite que todas las estaciones de trabajo y servidores restantes sean actualizados directamente sin necesidad del acceso constante a Internet, ya que el servidor es el único que se conecta descargando las actualizaciones y distribuyéndolas a los demás.

Servidor Proxy

Es el servidor que permite compartir el Internet a todos los usuarios de la institución y que a través del cual se aplican políticas de acceso para la navegación. Está instalado como sistema operativo Linux, la distribución Debian (Estándar de Software libre en la Institución) de 64 bits; se tiene instalado el servicio Squid y el paquete SARG, el cual permite monitorear los acceso a Internet por parte de los usuarios.

Servidores en General

Los Servidores tienen activos el Firewall respectivo sea en Windows o Linux; en el caso de Windows este lo posee internamente y es activado por las propiedades de las tarjetas de red, y en el caso de Linux este se lleva a cabo mediante el IPTABLES; También se tiene instalado los clientes de antivirus donde las definiciones de virus o huellas se actualicen a través del servidor de antivirus y por último estos deben estar a día con respecto a las actualizaciones de seguridad sean de Linux o Windows Update.

Existe varias herramientas para la administración remota de los Servidores en Windows y en Linux; en el caso de la institución se posee el RADMIN para la administración remota de los servidores en Windows y el Webmin para los servidores en Linux.

Estaciones de Trabajo

Las Estaciones de trabajo al igual que en los servidores, se tienen activos el Firewall que trae Windows XP u otro Firewall para otras versiones de Windows, este se realiza mediante las Directivas del Servidor de Dominio (Active Directory); También se tiene instalado los clientes de antivirus donde las definiciones de virus o huellas se actualicen a través del servidor de antivirus y por último estos estan al día con respecto a las actualizaciones de seguridad de Windows Update.

Servicios

Los servicios internos y externos estan protegidos a través de la implantación de Firewall en los Servidores que los posean, es decir, se activaron en el Firewall (Software) únicamente los puertos que usan dichos servicios. Es importante mencionar que los servicios Web aparte de la administración de los puertos requerido (80, 443), se tiene protegidos con el uso de contraseñas encriptadas y certificados de seguridad SSL.

Monitoreos

Uso de Internet a Usuarios Internos (Proxy)

Todos los usuarios del Rectorado/V.R. Bqto poseen acceso al correo electrónico interno, a los servicios web a nivel nacional de la UNEXPO, es decir, a cualquier URL que posea la cadena

unexpo.edu.ve, al igual que las página gubernamentales (.gob.ve o .gov.ve), www.bancodevenezuela.com (pago de nómina), algunas universidades nacionales y cualquier otra que sea necesaria para el cumplimientos de las labores de trabajo en la institución; cabe destacar que existe un grupo de usuario que posee acceso mediano a Internet (Sin pornografía, páginas de entretenimiento, descarga de archivos, etc), un grupo de usuario con acceso ilimitado(Internet full) y en las horas no laborables y fines de semana cualquier usuario posee acceso a Internet, por su puesto con las restricciones correspondientes. Por último, es importar señalar que todos estos controles se llevan a cabo mediante el servidor Proxy tomando en cuenta las IP y los grupos de usuarios definido en el Servidor de Dominio (Active Directory).

Acceso a Servidores públicos por parte de Usuarios Externos

Esto se logra a través de los LOGS de los servidores tanto en Linux (Archivos de texto editables, ubicados en /var/log/….) como en Windows (Visor de sucesos); Es necesario que todos los Servidores públicos (web, e-mail, ftp, DNS, etc..) tienen instalado como Sistema Operativo Gnu/Linux Debian.

Como sabemos, el tráfico generado en el acceso a los servicios públicos se realiza a través del Router de la institución, por lo tanto dicho tráfico es monitoreado en su totalidad gracias a la herramienta Netflow Analyzer 5.

Uso de carpetas compartidas y públicas (File Server y Estaciones de Trabajo).

Por norma, ninguna estación de trabajo debe tener compartida carpetas de forma local. Es importante mencionar que las carpetas compartidas se encuentran ubicadas en un Servidor de Archivo las cuales son resguardadas; Cabe destacar que dichas carpetas son monitoreadas para evitar el uso no institucional de las mismas.

Monitoreos de Aplicaciones instaladas en Servidores y/o Estaciones de Trabajo (TCPView).

Es necesario que cada vez que se vaya a instalar aplicaciones de terceros en estaciones de trabajo y/o servidores se verifique el funcionamiento de la misma, es decir, verificar si dicha aplicación no está generando tráfico en la red tanto interna como de Internet que pueda ocasionar problemas de seguridad; Este monitoreo se realiza de forma local (donde se esté instalando la aplicación) mediante la herramienta TCPView.

Sistema de respaldos

Se poseen respaldo de data en 3 niveles:

Nivel 1: Sistema RAID

RAID 0, RAID 1, RAID 1 + RAID 5, RAID5

Nivel 2: Respaldo en Cintas

Se posee respaldo en cintas Usando el software NTBACKUP

Nivel 3: Respaldo en CDs.

Se posee respaldo en **CDs**

Futuro a corto plazo

Firewall

La UNEXPO (Rectorado/VR Bqto) ya posee un Cisco ASA 5520(Firewall a nivel de hardware) el cual será instalado próximamente y nos permitirá reforzar la seguridad en toda la red del Campus; este dispositivo tendrá una conexión a toda la red de la UNEXPO (Bqto) por medio de la interfaz INSIDE la cual posee 100% de seguridad por defecto, también tendrá una conexión solamente a los servidores públicos de la institución mediante una interfaz llamada DMZ (zona desmilitarizada) y por supuesto una conexión a la red externa Wan.

Este dispositivo nos brinda el servicio de VPN para el acceso de usuarios remotos a la red interna. Por último, es importante señalar que las restricciones de acceso a los servicios, servidores, usuarios, etc se llevara a cabo a través de este dispositivo.

Futuro a Mediano y Largo plazo

Instalación de Red de Área de Almacenamiento SAN(Store Area Network)

Es una red independiente de almacenamiento de altas prestaciones basada en tecnología fibre channel . Su función consiste en centralizar el almacenamiento de los archivos en una red de alta velocidad y máxima seguridad, se trata de una solución global donde se comparte todo el área de almacenamiento corporativo.

Características Generales Servidor SAN:

- Chasis compacto de montaje en rack
- Desplazamiento con conexión directa o a través de Fibra Canal
- Desde 5 a 60 discos FC2 o ATA en expansión DAE2
- Hasta 64 servidores conectados a un solo array en SAN

Instalación de Cluster(agrupar) de Sistema Computacional

Un sistema paralelo o distribuido que consiste en la colección de computadoras totalmente interconectadas, que son utilizadas como un solo y unificado recurso computacional". En general, el objetivo de un cluster es hacer posible compartir carga computacional a lo largo de varios sistemas. Si falla un nodo, los otros le quitan su carga; si se necesita más capacidad, se pueden añadir más nodos Si falla cualquier componente del sistema, ya sea el Harware o el Software, el usuario puede notar, en todo caso una degradación del rendimiento, pero no notará una perdida de acceso al servicio.
Balanceo de Carga IP. Corre múltiples versiones de una aplicación y distribuye las peticiones entre diferentes versiones, de acuerdo con qué servidor es el menos cargado.

Implementación de una Infraestructura PKI

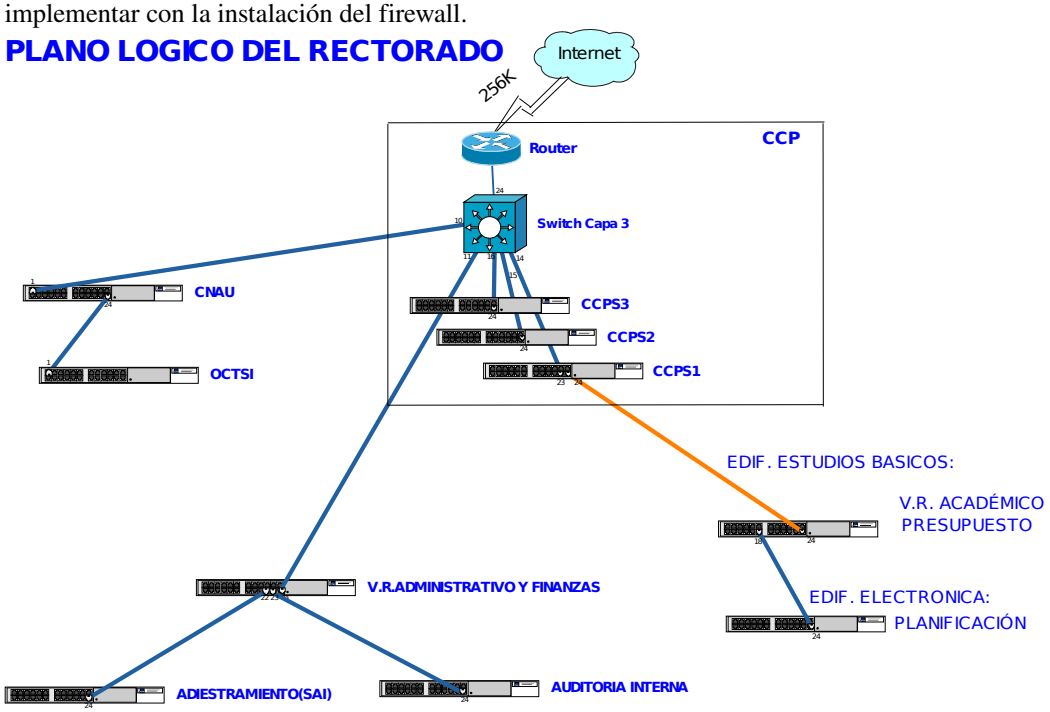
En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de

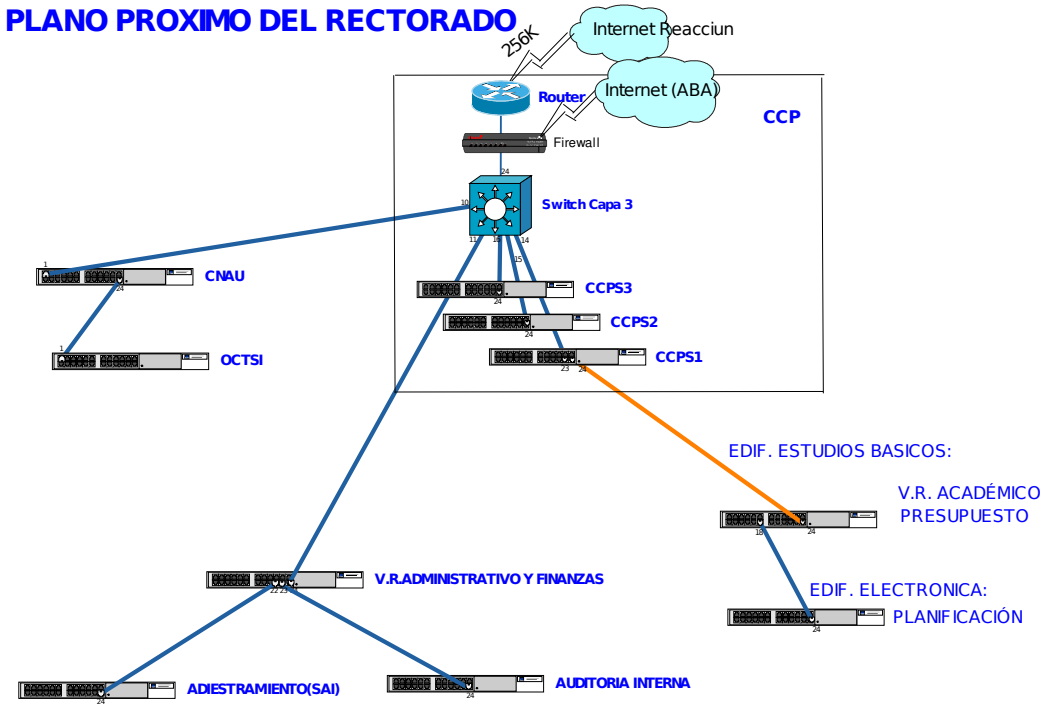
clave pública en comunicación electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

A continuación se muestra el plano lógico actual del Rectorado y el plano lógico próximo a implementar con la instalación del firewall.

PLANO LOGICO DEL RECTORADO



PLANO PROXIMO DEL RECTORADO



Anexo "R". Currículum Vítae del Autor

Datos Personales

- Nombres y Apellidos: Manuel Antonio, Mujica Ruiz
- Nacionalidad : Venezolano.
- Dirección : Barquisimeto Edo. Lara.
- Fecha de Nacimiento: 31 de julio de 1.971.
- E-Mail : mmujica@unexpo.edu.ve
- Web: www.mmujica.wordpress.com

Objetivo

Soy profesional del área de tecnología por más de 16 años, los últimos 3 años enfocado en el área de redes y seguridad además soy profesor universitario en el área de investigación e informática. El objetivo del presente currículum es presentar el historial de empleo, estudios y cursos realizados entre otros.

Historial de empleo

Coordinador Nacional de Tecnología de Información 2006-Actual

- Oficina Central de Tecnología y Servicios de Información, UNEXPO Barquisimeto-Edo. Lara.

Profesor 2005-Actual

- Universidad Nacional Experimental Simón Rodríguez, UNESR. Barquisimeto-Edo. Lara.
  - Asignaturas impartidas:
    Tecnológicas:
    - Teleproceso I
    - Gestión de Tecnología
    - Introducción al procesamiento de datos

    Investigación:
    - Proyecto I
    - Proyecto II
    - Seminario Especial de Grado.

Coordinador Nacional de Tecnología de Información 2006-2007

- Oficina Central de Tecnología y Servicios de Información, UNEXPO Barquisimeto-Edo. Lara.

Coordinador Nacional de Producción y Operaciones 2005-2006

- Oficina Central de Tecnología y Servicios de Información, UNEXPO Barquisimeto-Edo. Lara.

Coordinador de Informática 2003-2005

- Dirección de Investigación y Postgrado, UNEXPO Barquisimeto-Edo. Lara.

Coordinador de Informática 1996-2003

- Dirección de Investigación y Postgrado, UNEXPO Barquisimeto-Edo. Lara.

Programador 1992-1995

- Departamento de Programación, INCETA C.A., Los Teques-Edo. Miranda.

Profesor 1993-1994

- COMPUTACION TEXTO.TXT C.A, Los Teques-Edo. Miranda.

Programador 1991-1992

- TECNY GESTION 2.000 C., Los Teques-Edo. Miranda

Estudios

1990-1993 Colegio Universitario de Los Teques Cecilio Acosta "CULTCA", Los Teques- Edo. Miranda.

- **TSU Informática Índice: 7.30/9.00**

1999-2003 "Universidad Nacional Experimental "Simón Rodríguez" Bqto Edo. Lara.

- **Licenciado en Administración Mención Informática. Índice: 4.70/5.00**

1997-2001 "Universidad Nacional Experimental Politécnica Antonio José de Sucre" Barquisimeto Edo. Lara.

- **Especialista en Logística Industrial. Índice: 18.50/20**
- **Mención: Cumlaude**

2003-2004 Universidad Pedagógica Experimental Libertador, Bqto Edo. Lara.

- **Diplomado en capacitación Pedagógica para Profesionales no Docentes. Índice: 10/10.**

2003-2004 Universidad Centro-Occidental Lisandro Alvarado, Bqto Edo. Lara.

- **Maestría en Ciencias de la Computación, Mención: Redes de Computadores, (Tesista). Índice: 18,2/20**

Cursos Realizados

- Introducción a los sistemas operativos, Tecny Gestión 2.000 c.a.,16 Hrs.,1.990
- Programación en COBOL, PASCAL, Tecny Gestión 2.000 c.a.,192 Hrs.,1.990-1.991
- Programación en,Tecny Gestión 2.000 c.a.,96 Hrs.,1.991
- Principios de hyper-programación, modelaje de datos y herramientas case, Tecny Gestión 2.000 c.a. y Fundaca, 18 Hrs., 1.991
- Calidad y tecnología para afrontar el reto gerencial de los 90,Tecny Gestión 2.000 c.a.,16 Hrs.,1.991
- Hábitos de estudios, Centro de orientación profesional y educativa.,64 Hrs.,1.993
- Dirección de reuniones, Relaciones humanas, Programa desarrollo del pensamiento, I.N.C.E.,64 Hrs.,1.993-1.995
- Principios básicos de higiene industrial, salud y seguridad ocupacional, Administradora Lockey,20 Hrs.,1.995
- Electricidad: Instalaciones de la casa,A.V.E.C.,300 Hrs.,1.995
- Sql Windows Básico, UNEXPO – Barquisimeto,40 Hrs.,1.997
- Taller Calidad total e inteligencia intuitiva,UNEXPO – Barquisimeto,08 Hrs.,1.998
- Mantenimiento productivo total, UNEXPO – Barquisimeto,04 Hrs.,1.998
- Elaboración de Normas y Procedimientos , Taller Formación de Equipos de Trabajos.,UNEXPO – Barquisimeto,08 Hrs.,1.998
- Manejador de base de datos SQL-SERVER, Operación de micro básico (MS-PROJECT), I.N.C.E.,60 Hrs.,1.999
- Fundamento de las tecnologías de redes, UCLA, 18 Hrs.,2.003
- Modelaje de sistemas de software, UCLA, 18 Hrs.,2.003
- II Jornadas de Investigación y Postgrado,UNEXPO – Barquisimeto,--,2.004
- Diseño e implementación de Protocolos de Comunicación y Aplicaciones Multimedia Orientado a QoS.,UCLA,--,2.004
- Inteligencia Artificial, UNEXPO – Barquisimeto,48 Hrs.,2.005
- Festival Latinoamericano de Software Libre, Fundacite Lara – MCT - UCLA,--,2.005.
- Redes de Computadores, UNEXPO, 48 Hrs., 2.004
- Protocolos de Comunicaciones, UNEXPO, 48 Hrs., 2004
- Redes de Alta Velocidad, UNEXPO, 48 Hrs., 2.005
- Gerencia de Organizaciones, UNEXPO, 48 Hrs. 2.005
- Gerencia de Proyectos, UNEXPO, 48 Hrs. 2.005
- Fundamentos en Linux, CADIF1, 14 Hrs. 2.005
- II Encuentro Universidad-Gobierno-Sector Productivo, UNEXPO, 2.005
- I Encuentro de Tecnología y Servicios de Información UNEXPO, 2.005

- La Academia Latinoamericana de Seguridad Informática, Modulo 1 – 7, Microsoft TechNet , 2.005
- Taller de DNS (Domain Name Service), MCT-CNTI, 24 Hrs., 2.006
- Software Libre nivel 0 y 1, MCT-Fundacite-ASL, 172 Hrs., 2.006
- Formación de auditores de Sistemas de Gestión de Seguridad de la Información ISO 27001:2005, FONDONORMA, 36 Hrs., 2.006
- Fundamentos de Seguridad en redes de Datos, 40 Hrs., 2.006

Jurado de Tesis

- Diseño de un software integrado de control de personal dirigido al departamento de recursos humanos del hospital central Dr. Placido Daniel Rodriguez Rivero de San Felipe orientado a software libre., UNESR, 2006

- Propuesta de un sistema de información catastral de administración de redes de aguas blancas y servidas para Hidrolara, UNESR, 2006