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

DISEÑO DE UNA METODOLOGIA PARA EL ANALISIS DE RIESGO EN LOS SISTEMAS DE GESTION DE SEGURIDAD DE INFORMACION (MARISGSI) EN LAS UNIVERSIDADES DE BARQUISIMETO ESTADO LARA

Barquisimeto, enero de 2013

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

DISEÑO DE UNA METODOLOGIA PARA EL ANALISIS DE RIESGO EN LOS SISTEMAS DE GESTION DE SEGURIDAD DE INFORMACION (MARISGSI) EN LAS UNIVERSIDADES DE BARQUISIMETO ESTADO LARA

Título de grado presentado como requisito parcial para optar al grado de Magister Scientiarum en Ciencias de la Computación

AUTORA: Ing. Yenny Maribel Alvarez Sosa
TUTOR: Lic. Manuel Mujica

Barquisimeto, enero de 2013

DISEÑO DE UNA METODOLOGIA PARA EL ANALISIS DE RIESGO EN LOS SISTEMAS DE GESTION DE SEGURIDAD DE INFORMACION (MARISGSI) EN LAS UNIVERSIDADES DE BARQUISIMETO ESTADO LARA

Por: Yenny M. Alvarez Sosa

Trabajo de Grado aprobado

_____ _____

Jurado 1 Jurado 3

_____

Jurado 2

Barquisimeto, _____ de _____ de 2012

DEDICATORIA

A mis hijos Carla y José, por ser lo más grande que Dios me ha regalado en esta vida, por ser esos seres tan maravillosos que le ponen, día a día, color a mi existencia, llenándome de situaciones hermosas de aprendizaje y otorgándome fuerza y voluntad para seguir adelante.

AGRADECIMIENTO

Primeramente, a Dios por dejarme existir, por permitir que su sabiduría dirija y guie mis pasos en cada momento.

Al Lic. Manuel Mújica, por su paciencia, dedicación, comprensión, amistad, energía transmitida, orientación, confianza y apoyo en este largo camino.

A la Sra. Consuelo Romero, por brindarme su apoyo y colaboración con mis hijos para poder asistir a mis clases y terminar mi escolaridad.

INDICE GENERAL

p.

LISTA DE CUADROS

Cuadro **p.**

LISTA DE GRÁFICOS

Gráfico **p.**

LISTA DE FIGURAS

Figura **p.**

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

DISEÑO DE UNA METODOLOGIA PARA EL ANALISIS DE RIESGO EN LOS SISTEMAS DE GESTION DE SEGURIDAD DE INFORMACION EN LAS UNIVERSIDADES DE BARQUISIMETO ESTADO LARA (MARISGSI)

Autora: Yenny Maribel Alvarez Sosa
Tutor: Manuel Mujica
Fecha: enero de 2013

RESUMEN

Las organizaciones hoy día, con la tecnología y complejidad en el manejo de la información, donde enfrentan diferentes amenazas que explotan sus vulnerabilidades en el dominio de la confidencialidad, integridad, disponibilidad y el no repudio de la información en la empresa, es primordial para el aumento de su competitividad el resguardo de estos dominios. La presente investigación propone una Metodología para el Análisis de Riesgos en las Universidades de Barquisimeto Estado Lara, con el objetivo de mitigar los riesgos para aumentar la productividad operacional y mantener disponibles los servicios de tecnología que ofrecen a su comunidad estudiantil. Para ello se realizó: a) un diagnóstico en las universidades UCLA, UPEL, UNEXPO, UNA, UNY, UNESR y UFT para determinar si usan algún procedimiento metodológico para realizar los análisis de riesgos a sus SGSI, b) una comparación de las metodologías OCTAVE, MAGERIT, EBIOS, CRAMM y MEHARI para obtener los criterios más idóneos para la propuesta metodológica y c) se diseñó la propuesta usando los criterios obtenidos en la comparación y tomando en cuenta los requerimientos que ofrece las normas ISO/IEC 27002:2005 e ISO/IEC 27005:2008. La metodología aplicada es de proyecto especial y se apoya en un diseño de investigación no experimental con un nivel descriptivo y una investigación de campo. Finalmente, la metodología propuesta consistió en identificar los activos más críticos de las instituciones, valorarlos y codificarlos, identificar las amenazas a las que se encuentran expuestos dichos activos, identificar las vulnerabilidades y determinar cuáles son los controles pertinentes para minimizar el riesgo.

Palabras claves: Seguridad de información, análisis de riesgos, amenazas, vulnerabilidades, Sistemas de gestión, OCTAVE, MEHARI, CRAMM, MAGERIT, EBIOS, ISO/IEC 27002:2005, ISO/IEC 27005:2008.

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

DESIGN METHODOLOGY FOR RISK ANALYSIS SYSTEM FOR INFORMATION SECURITY MANAGEMENT IN UNIVERSITIES OF BARQUISIMETO STATE LARA (MARISGSI)

Author: Yenny Maribel Alvarez Sosa
Tutor: Manuel Mujica
Date: January 13

ABSTRACT

Organizations today, with the technology and complexity of information management, which face different threats that exploit vulnerabilities in the domain of the confidentiality, integrity, availability and non-repudiation of information on the company, it is essential for increased competitiveness the receipt of these domains. This research proposes a methodology for Risk Analysis at the Universities of Barquisimeto, Lara State, in order to mitigate risks to increase operational productivity and maintain available technology services offered to its student community. This was achieved by: a) a diagnosis UCLA, UPEL, UNEXPO, A, UNY, UFT UNESR and to determine if any methodological procedure used to perform risk analyzes their ISMS, b) a comparison of methodologies OCTAVE , MAGERIT, EBIOS, and MEHARI CRAMM for the most appropriate criteria for the methodology and c) the proposal was designed using the criteria obtained in the comparison and taking into account the requirements offering ISO / IEC 27002:2005 and ISO / IEC 27005:2008. The methodology is of special project and is supported by a non-experimental research design with a descriptive level and field research. Finally, the proposed methodology is to identify the most critical assets of institutions, assessing and code, identify the threats they are exposed such assets, identify vulnerabilities and determine appropriate controls to minimize the risk.

Descriptors: Information Security, risk analysis, threats, vulnerabilities, management systems, OCTAVE, MEHARI, CRAMM, MAGERIT, EBIOS, ISO/IEC 27002:2005, ISO/IEC 27005:2008.

INTRODUCCION

Las organizaciones hoy día, con la tecnología y complejidad en el manejo de la información, donde enfrentan diferentes amenazas que explotan sus vulnerabilidades en el dominio de la confidencialidad, integridad, disponibilidad y el no repudio de la información en la empresa, es primordial para el aumento de su competitividad el resguardo de estos dominios; por lo que están obligadas, si desean continuar operando, a establecer SGSI que permitan identificar sus activos vitales de información, e implantar los controles pertinentes. Por lo tanto, es importante establecer el proceso de análisis de riesgos para identificar los activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para mitigar la ocurrencia del riesgo.

Aunado a ello, es fundamental conocer que el análisis de riesgo es crucial para el desarrollo y operación de un SGSI, ya que justo en esta etapa es donde la organización debe construir su "modelo de seguridad", que no es más que la representación de todos sus activos y sus dependencias jerárquicas, así como, todo aquello que pudiera ocurrir (amenazas) y que tuviera un impacto en la organización.

Es importante considerar el análisis de riesgo como el núcleo de toda organización en cuanto a la seguridad de la información, el cual permite establecer un nivel adecuado de seguridad, que se aspira lograr en la protección de los activos, de qué o quién protegerlos y cómo hacerlo, teniendo como guías las normas de la ISO[1] (Organización Internacional de Estandarización) e IEC[2] (Comisión Electrotécnica Internacional) las cuales forman el sistema especializado para la estandarización mundial; entre estas están la norma ISO/IEC 27005:2008, que proporciona directrices

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

[2] *International Electrotechnical Commission (IEC),* es la organización líder a nivel mundial encargada de preparar y publicar normas internacionales para todas las tecnologías eléctricas, electrónicas y afines. http://www.iec.ch

para la gestión del riesgo de seguridad de la información en una organización; sin embargo, esta norma no proporciona ninguna metodología específica para el análisis y gestión del riesgo de la seguridad de la información, la norma ISO/IEC 27002:2005, antigua ISO/IEC 17799, que establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización, donde los objetivos de control y los controles son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo.

La presente investigación se orientó en la búsqueda y elaboración de un modelo metodológico para realizar el proceso de análisis de riesgos en los Sistemas de Gestión de Seguridad de Información (SGSI[3]), que son manejados por las universidades UCLA, UNEXPO, UNA, UPEL, UNESR, UNY y UFT de Barquisimeto, con el fin de asegurar el activo fundamental de sus sistemas como lo es la información, permitiendo identificar las amenazas y vulnerabilidades a las que se encuentra expuesto dicho activo, valorando el impacto que supondría en la institución dicha materialización y estableciendo los controles necesarios para mitigar el riesgo.

De igual manera, se tienen como guía las metodologías para el análisis de riesgos internacionales como MAGERIT, OCTAVE, CRAMM, EBIOS y MEHARI.

En este sentido, el trabajo de investigación se estructura en seis (VI) capítulos de la siguiente manera:

Capítulo I: El problema de investigación, en el cual se plantea de forma clara, precisa tanto la incidencia del problema como los objetivos de la investigación, justificación e importancia, alcance y limitaciones.

Capítulo II: Denominado marco Teórico, contentivo de los antecedentes de investigación, bases teóricas y legales en relación con el objeto de estudio.

Capítulo III: Llamado marco Metodológico, donde se describe la metodología usada en la investigación, el diseño de la investigación, población y muestra,

[3] **Sistema de Gestión de Seguridad de la Información (SGSI)**,esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. ISO/IEC 27001:2005

instrumentos de recolección de datos, validez y confiabilidad de los instrumentos de recolección de datos.

Capítulo IV: Corresponde al análisis de los datos obtenidos en los instrumentos.

Capítulo V: En este capítulo se presenta el diseño de la metodología para el análisis de riesgos en los SGSI de las universidades de Barquisimeto Estado Lara.

Capítulo VI: Se expresan las conclusiones a las que se llegó conforme a los objetivos planteados, así como también, aquellas recomendaciones pertinentes de la investigación.

Finalmente, se presentan las referencias bibliográficas y los anexos.

CAPITULO I

EL PROBLEMA DE LA INVESTIGACION

Planteamiento del problema

En la actualidad la seguridad de la información es un punto clave de análisis, puesto que las condiciones van cambiando a lo largo del tiempo de acuerdo a las nuevas tecnologías, por lo que la posibilidad de interconectarse a través de diversas redes, ha permitido ahondar en nuevos horizontes para conocer más allá de lo que podemos observar en nuestro país, dando como resultado, la aparición de nuevas amenazas tecnológicas que pudieran poner en riesgo los activos de información.

En este orden de ideas, Palma (2007) define la seguridad de la información como la protección de la información de un rango de amenazas para poder asegurar la continuidad de la organización, minimizar riesgos y maximizar operatividad y eficiencia y resulta oportuno destacar que no es igual a la seguridad informática.

Debido a lo anteriormente expuesto, muchas instituciones tanto públicas como privadas, han tomado en cuenta la necesidad de desarrollar procedimientos que indiquen el uso adecuado de las herramientas tecnológicas y recomendaciones para obtener el mayor beneficio de éstas, y evitar el uso indebido de la mismas, lo cual puede traer como consecuencia serios problemas en los activos de la organización.

En este sentido, la información, junto a los procesos, personas y sistemas que hacen uso de ella, son activos muy importantes dentro de una organización, donde la confidencialidad, integridad, disponibilidad y no repudio de información son elementos esenciales para mantener los niveles de competitividad, rentabilidad y

conformidad legal necesarios para lograr los objetivos de la entidad. Ahora bien, la disponibilidad es la "propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada" (ISO/IEC 27001:2005, p. 9), la confidencialidad es la "propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados", la integridad es la "propiedad de salvaguardar la exactitud e integridad de los datos" (ISO/IEC 27001:2005, p. 10) y el no repudio "proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje u originado o haber sido el destinatario de una acción" (Daltabuit y otros, 2007, p. 104).

Por lo tanto, deben existir técnicas y métodos que la aseguren, más allá de la seguridad física que se pueda establecer en los equipos en los cuales se almacena. De esta manera, algunas técnicas de prevención las brinda la seguridad lógica mediante la aplicación de procedimientos que resguarden el acceso a los datos y sólo permiten acceder a ellos a las personas, procesos o entidades autorizadas para hacerlo.

En este sentido, las instituciones de educación superior tanto públicas como privadas y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, inherentes a los activos, pueden someter a los mismos a diversas formas de fraude, espionaje, sabotaje o vandalismo, robos de información, pérdidas de datos importantes, ausencia de políticas de seguridad, virus, hacking, ataques de negación de servicio, entre otros. También, se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia entidad o aquellos provocados por catástrofes naturales y fallas técnicas; tales aspectos están contemplados en la Ley Especial de Delitos Informáticos de nuestro País, por lo que, las universidades deben cumplir con este marco legal.

Cabe destacar, que dentro del campo de la seguridad de la información se encuentra un aspecto de suma importancia como lo es el proceso de Análisis de Riesgos; entendiendo por riesgo "la combinación de la probabilidad de un evento y sus consecuencias" ISO/IEC 27002:2005 (p. 14), así como también lo expresa Aceituno (2006), la posibilidad de que se produzca un impacto determinado de un

activo en un dominio o en toda la organización. De las definiciones anteriores, se infiere que riesgo es toda probabilidad de que una amenaza ocurra durante un período definido ocasionando impactos económicos, materiales, personales y organizacionales.

En este orden de ideas, el análisis de riesgo lo define la norma ISO/IEC 27002:2005 como el "uso sistemático de la información para identificar las fuentes y calcular el riesgo" (p. 14), por lo tanto, es crucial para el desarrollo y operación de un SGSI, ya que en esta etapa es donde la organización debe construir su "modelo de seguridad", es decir, la representación de todos sus activos y sus dependencias jerárquicas, así como, todo aquello que pudiera ocurrir (amenazas) y que tuviese un impacto en la organización.

Por otro lado, un SGSI es un Sistema de Gestión de Seguridad de la Información o ISMS por sus siglas en inglés (Information Security Management System) y consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por la organización; de esta forma, la norma ISO/IEC 27001:2005 lo define como "esa parte del sistema gerencial, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información" (p. 10); así como también especifica que el sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos.

En este sentido, el propósito de un SGSI no es garantizar la seguridad sino garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la entidad de una forma documentada, sistemática, estructurada, continua, eficiente y adaptada a los cambios que se producen en la organización, los riesgos, el entorno y las tecnologías.

Con respecto al análisis de riesgos, se puede inferir que es un elemento fundamental para determinar las medidas de seguridad de un activo, sistema, o lo que se esté analizando, ya que identifica los riesgos, amenazas y vulnerabilidades y estima el impacto potencial que supone su propia destrucción o la pérdida de

disponibilidad, confidencialidad e integridad de la información; por lo que, impacto es definido por la metodología MAGERIT V. 2 (2006) como:

> La medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que éstas tendrían sobre el sistema (p. 23).

Esto en concordancia con lo planteado por Royal (1998), quien expresa que:

> No todas las exposiciones necesitan ser o deberían ser controladas, el control total no es un costo eficaz y generalmente es muy ineficiente, sin embargo, si el diseñador no tiene idea de que la exposición presenta el mayor riesgo en términos de frecuencia de ocurrencia y costo, no tiene otra alternativa que controlar cada exposición (p. 83).

Por otro lado, Alberts y Dorofree (2003), explican que se deben crear registros de los impactos potenciales que pueden derivarse de las amenazas de los activos, por lo que se debe establecer un vínculo entre los activos, las amenazas y los objetivos de negocio de la organización, que proporcionan una base sobre la que analizar los riesgos.

En consecuencia, deben existir procedimientos o métodos para realizar el proceso de análisis de riesgos en las instituciones que permitan identificar las amenazas, las vulnerabilidades asociadas, determinar el impacto en caso de su materialización, obtener el riesgo al que se está expuesto y como lo expone Alberts y Dorofree (2003) “tomar decisiones en relación a que riesgos la organización aceptará y que controles serán implantados para mitigar el riesgo”.

En este sentido, la problemática presentada, según información recabada a través de entrevistas informales no estructuradas a los administradores de red de las instituciones UCLA, UNEXPO, UNA, UNESR, UNY, UFT y UPEL es la siguiente: ausencia de políticas de seguridad por falta de presupuesto y coordinación gerencial, hackeos a servidores web y de correo electrónico, falta de adiestramiento al personal, fallas eléctricas, fraude en el sistema de pagos, virus, phising, negación de servicio, pérdida de datos, manipulación de la información por los usuarios, hurto, usuarios que quieren acceder al servidor principal, personas que se hacen pasar por otras en

registro académico, etc., lo cual trae como consecuencia la interrupción en los servicios ofrecidos a las comunidades estudiantiles, mal funcionamiento de los procesos estructurales, detención de los servicios en la red, etc., generando un impacto operativo y económico en las instituciones que no está siendo evaluado por carencia de procedimientos para mitigar los riesgos que son generados por los incidentes antes mencionados. Por lo que es necesario, que los responsables de la seguridad de la información en conjunto con la directiva de las universidades, tomen conciencia y deban contrarrestar los riesgos a los que están sometidos sus activos principales.

De lo antes expuesto, surge la necesidad de diseñar una metodología para análisis de riesgos en los Sistemas de Gestión de Seguridad de la Información (SGSI) de las universidades de Barquisimeto Estado Lara (MARISGSI).

En vista de los argumentos antes señalados, surgen las siguientes interrogantes de la investigación:

¿Cuáles son las especificaciones del proceso de análisis de riesgos en cuanto a los Sistemas de Gestión de Seguridad de la información actuales en las universidades de Barquisimeto Estado Lara?

¿Cuáles son los criterios pertinentes para elaborar una metodología para análisis de riesgos en los SGSI tomando en cuenta las metodologías CRAMM, MAGERIT, EBIOS, OCTAVE y MEHARI?

¿Cuál es el procedimiento óptimo para realizar el proceso de análisis de riesgos en los SGSI de las universidades de Barquisimeto Estado Lara?

Cada una de las interrogantes anteriores se les dará respuesta en el desarrollo del presente estudio.

Objetivos de la investigación

Objetivo general

Diseñar una metodología para el análisis de riesgos en los Sistemas de Gestión de Seguridad de Información (SGSI) en las Universidades de Barquisimeto Estado Lara (MARISGSI).

Objetivos específicos

- Diagnosticar la situación real con respecto al proceso de análisis de riesgos en las Instituciones Universitarias de Barquisimeto Estado Lara.
- Comparar las metodologías existentes para el Análisis de Riesgos en los SGSI.
- Proponer una Metodología para el Análisis de Riesgos en los SGSI para las Universidades de Barquisimeto Estado Lara.

Justificación e importancia

Las universidades de Barquisimeto, al igual que cualquier organización usan los sistemas de información para su operatividad, convirtiéndose en un activo fundamental que necesita asegurarse ante las amenazas que hoy día afectan su disponibilidad, integridad, confidencialidad y no repudio que son esenciales para lograr sus objetivos, aumentando los riesgos y causando grandes daños operativos y económicos.

En este sentido, se deben establecer procedimientos adecuados y controles de seguridad basados en el análisis de riesgos para conocerlos y afrontarlos de manera adecuada, para lograr reducir las amenazas hasta alcanzar un nivel asumible por las instituciones, disminuir los costos derivados de una racionalización de los recursos y asegurar el cumplimiento de la normativa legal de nuestro País, por lo cual, se debe contar con el apoyo de toda la institución.

Con la propuesta de esta metodología para el Análisis de Riesgos en los SGSI se espera ofrecer una solución para que las instituciones tanto públicas como privadas, dispongan de un método que les permita identificar cuáles son sus activos primordiales, cuáles son las amenazas que afectan a dichos activos, cuáles son las vulnerabilidades existentes y de esta manera determinar cuál es el impacto que tendrá la institución si esas amenazas se materializan y establecer los controles necesarios para mitigar los riesgos encontrados.

De igual manera, se espera que la investigación sirva como base para futuras investigaciones en el área, así como aportar una alternativa para el resto de las universidades u organizaciones con problemática similar.

Alcances

La investigación permitirá definir el procedimiento para realizar un análisis de riesgo a los SGSI donde se garantice mitigar los riesgos en los activos de información que son fundamentales para las instituciones universitarias tanto públicas como privadas de Barquisimeto.

En este sentido, la metodología se fundamenta en la norma ISO/IEC 27005:2008 y contempla los criterios de identificación de activos, amenazas y vulnerabilidades, así como la determinación del impacto de que se materialicen las amenazas en los activos de las instituciones y el establecimiento de los controles adecuados.

Cabe destacar, que la propiedad no repudio de la información es tomada en cuenta en esta metodología, como una dimensión más de seguridad, ya que permite probar la participación de las partes en una comunicación y por estar incluida dentro de la Ley de mensaje de datos y firmas electrónicas de nuestro País.

Además, la metodología anexa en el proceso de análisis de riesgos los indicadores de Impacto y Salvaguardas (controles), los cuales no son tomados en cuenta en las metodologías estudiadas, ya que forman parte del proceso de gestión de riesgos (evaluación de los riesgos).

Limitaciones

La investigación abarcará solo la propuesta de la metodología para análisis de riesgos, donde quedará por parte de las instituciones la implementación y realizar el proceso de evaluación de los riesgos.

Por otro lado, la presente metodología toma en cuenta sólo los activos de información.

CAPITULO II

MARCO TEORICO DE LA INVESTIGACION

Antecedentes de la investigación

En toda investigación debe realizarse una revisión bibliográfica sobre los temas involucrados, a continuación se citan investigaciones que han contribuido a generar antecedentes a la propuesta de diseñar una metodología de análisis de riesgos en los Sistemas de Gestión de Seguridad de la Información en las Universidades de Barquisimeto Estado Lara. Entre las investigaciones que sirvieron de apoyo como antecedentes al estudio planteado, se encuentran:

Mendoza (2010), presenta en su tesis de maestría, el diseño de un *Sistema de Gestión para la Seguridad de la Información para el Centro de Tecnología de Información y Comunicación del Decanato de Ciencia y Tecnología – UCLA*, basado en la fase de planeación de la norma ISO/IEC 27001:2005 y en los controles de la norma ISO/IEC 27002:2005, como metodología de análisis de gestión del riesgo se empleó MAGERIT v 2.0 y la herramienta ISO27K de la ISO 27001 Security Home. La investigación se enmarco en la modalidad de proyecto factible, y tiene como resultado reducir el riesgo en el SGSI hasta un nivel aceptable al implantar los controles que se proponen como correctivo.

Esta investigación tiene relación con el presente estudio, porque toma como referencia la metodología española MAGERIT para el analisis de riesgos en una institución publica de educación superior, además se apoya en los controles de la norma ISO/IEC 27002:2005, como directriz para el proceso de análisis de riesgos.

El artículo de la revista Enl@ce Vol. 6 (1) 2009, en las páginas 43-55, por De Freitas (2009) con el título "*Análisis y Evaluación del Riesgo de la Información: caso de estudio Universidad Simón Bolivar",* el cual tiene como objetivo conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información que estan en custodia en la Dirección de Servicios Telemáticos (DST) de la Unviersidad Simón Bolivar ubicada en Caracas, Venezuela, con el fin de sugerir estrategias que minimicen la ocurrencia de posibles amenazas que en la mayoría de los casos explotan las vulnerabilidades organizacionales. Basado en una metodología de estudio de caso, este estudio permito recoger información detallada usando una variedad de sistemas de recolección de datos, como entrevistas semiestructuradas, estructuradas y en profundidad, revisión bibliográfica y arqueo de fuentes. Igualmente se realizaron visitas a las instalaciones de la dirección evaluada y se revisaron aspectos de seguridad física previstos en la norma ISO 27001:2007.

Se concluye que cada uno de los elementos en custodia de la DST es de suma importancia para la Universidad Simón Bolivar, por lo que se sugiere la aplicación de algunos controles establecidos en las normas ISO, para cada uno de dichos activos.

La metodología presentada por De Freitas, establece conceptos claros y precisos concernientes al análisis de riesgos, métodos para el cálculo del riesgo, en el sector universitario Venezolano; así como también puntos claves con respecto a la metodología OCTAVE, información relevante para el desarrollo de la metodología elaborada.

Matalobos (2009), en su trabajo de grado *"Análisis de riesgos de seguridad de la información",* realiza un proceso de análisis de riesgos definiendo una metodología de trabajo desarrollada a medida y basada en las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de la información y en las necesidades, cultura y estrucutra específicas de la organización; que permitió cuantificar y comparar los requerimientos de seguridad de la información de la organización con los controles implantados para su cumplimiento, y, en base a las diferencias encontradas, se definieron los controles adicionales necesarios para cumplir todos los requerimientos. Aunado a esto, diseñó y desarrolló una herramienta

informática de soporte, que permitió aplicar la metodología de forma eficaz y eficiente.

Por lo que, la investigación realizada por Matalobos, ofrece a la presente investigación aportes importantes sobre el funcionamiento de los procesos de los estandares internacionales y las metodologías para realizar un análisis de riesgos en cualquier organización. Además, aporta un procedimiento para la selección de criterios para el diseño de una metodología propia basandose en algunas metodologías comerciales internacionales para el análisis de riesgos.

Méndez (2008), en su tesis de grado "*Propuesta de un plan estratégico que oriente la búsqueda de políticas de seguridad en la información para la Corporación Venezolana Agraria"* siendo el enfoque principal garantizar la integridad, disponibilidad y confidencialidad de los datos generados, procesados y almacenados en la red corporativa de la Corporación Venezolana Agraria.

La metodología usada fue la modalidad de proyecto especial, investigación de campo, de carácter descriptiva y constó de dos fases: diagnóstico y diseño de la propuesta, donde el resultado fue el plan estratégico para dar a conocer los riesgos que conlleva la información de la organización, permitiendo crear políticas de seguridad para establecer un canal formal de actuación de los usuarios en relación con los recursos y servicios importantes de la empresa.

En este sentido, la investigación de Méndez contribuye al estudio actual en que queda demostrado que toda organización debe mantener su activo principal, como lo es la información, en un nivel de seguridad alto, disminuyendo los riesgos a través de la identificación de amenazas y vulnerabilidades de dicho activo. Por lo que las organizaciones deben crear sus políticas de seguridad y aplicar análisis de riesgos en los períodos de tiempo que lo consideren necesario, así van logrando mantener una seguridad alta y sus activos actualizados. Igualmente, presenta bases teóricas concernientes al análisis de riesgos, así como también, el procedimiento general para realizar tal proceso.

Berenguela y Cortes (2006), en su tesis de grado *"Metdología de medición de vulnerabilidades en redes de datos de organizaciones"* presentan la creación de una

metodología para medir la seguridad de redes de datos que facilite al administrador de red conocer las vulnerabilidades de esta, y que se obtenga la información suficiente para crear políticas de seguridad que minimicen o eliminen todos los posibles riesgos; usando una metodología empírico-análitica debido a que es un sistema auto correctivo y progresivo; es decir, la metodología esta abierta a la incorporación de nuevos conocimientos y procedimientos. Para evaluar la metodología usaron la institución INACAP (Universidad Tecnológica de Chile); y como resultado luego de realizar el proceso de análisis de riesgos que plantea la metodología creada, se obtuvo datos que cuantificados permitieron crear gráficos para observar facilmente el grado de seguridad en la que se encuentra la institución, cuyo resultado fue de un 29%; concluyendo que INACAP presentaba una bajo grado de vulnerabilidad, lo que no implica que esté completamente segura, porque si algunas de estas vulnerabilidades eran detectadas por atacantes, el sistema se podia ver completamente comprometido y para ello recomendaron seguir algunas politicas y sugerencias para disminuir las vulnerabilidades existentes.

El trabajo de investigación presentado por Berenguela y Cortes aportó a la presente investigación, una serie de criterios que se deben tomar en cuenta para crear una metodología usando el análisis de riesgos para encontrar vulnerabilidades y cuantificarlas para determinar el grado de seguridad de cualquier organización.

Bases Teóricas

Dentro de las perspectivas teóricas que sustentan esta investigación, se ha considerado el estudio de los temas sobre: seguridad de la información, normalización de la seguridad de la información, Sistemas de Gestión de Seguridad de la Información (SGS), amenazas, vulnerabilidades, riesgos, impacto, análisis de riesgos, ISO/IEC 27005:2008 y metodologías para el análisis de riesgos.

Seguridad de la información

Seguridad

Definida por la Real Academia Española (RAE) como "cualidad de seguro" y **seguro** como "libre y exento de todo peligro, daño o riesgo"; por lo que se puede decir entonces que seguridad, es la ausencia de riesgo o la confianza en algo o alguien. Pero el término seguridad es muy amplio y puede tomar diversos sentidos dependiendo del área a la que haga referencia.

Información

Entre las definiciones generales de información se encuentra la contenida en la RAE que la define como "acción y efecto de informar", así como **informar** es "enterar, dar noticia de algo".

Por otro lado, en el área de la informática la Norma ISO/IEC 27002:2005, define **información** como "un activo, que como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido" (p. 9). Por lo tanto, mantenerla segura es fundamental en el funcionamiento de cualquier empresa, ya que actualmente con la creciente interconectividad, está expuesta a una gran cantidad y variedad de amenazas y vulnerabilidades; por lo que, al encontrarse insegura las organizaciones no podrán avanzar hasta el punto de llegar a desaparecer en el mercado; como por ejemplo, lo ocurrido en las Torres Gemelas el 11 de Septiembre del 2.001 en la ciudad de Nueva York, o el incendio del Edificio Windsor de Madrid el 13 de Febrero del 2.005, donde las grandes organizaciones que allí se encontraban desaparecieron debido a la pérdida masiva de información. Es por esto, que hoy en día contemplar la seguridad de los Sistemas de Gestión de Seguridad de la Información (SGSI) es un elemento

fundamental, no sólo para garantizar el futuro de las organizaciones, sino además para proporcionar a los clientes productos y servicios fiables.

La información se encuentra disponible en varias formas, puede estar impresa, guardada electrónicamente, mostrada en películas, hablada en alguna conversación, o en cualquier otra forma, por lo que sin importar su presentación debe protegerse de cualquier amenaza, para garantizar la confidencialidad, integridad, disponibilidad y no repudio.

Seguridad de la información

Desde el surgimiento de la raza humana en el planeta, la información estuvo presente bajo diversas formas y técnicas. El hombre buscaba representar sus hábitos, costumbres e intenciones en diversos medios que pudiesen ser utilizados por él y por otras personas, además de la posibilidad de ser llevados de un lugar a otro. La información valiosa era registrada en objetos preciosos y sofisticados, pinturas magníficas, entre otros, que se almacenaban con mucho cuidado en locales de difícil acceso, a cuya forma y contenido sólo tenían acceso quienes estuviesen autorizados o listos para interpretarla.

Actualmente, la información es el objeto de mayor valor para las organizaciones y generar confianza es un objetivo clave para las mismas, lo cual se logra implementando seguridad en la información que manejan para dar respuesta a un entorno dinámico y cambiante, por lo que deben implantar la **seguridad** como un proceso que integre los aspectos de la seguridad física y lógica de los SGSI con el fin de minimizar los riesgos que pueden impactar en el negocio y la operatividad de la organización, es así que la norma ISO/IEC 27002:2005 define la **seguridad de información** como “la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales” (p. 9).

Además, es importante recalcar que un plan de seguridad de la información debe contemplar como base fundamental, como lo indica la norma ISO/IEC 27001:2005, la "preservación de la confidencialidad, integridad y disponibilidad de la información" (p. 10), así como también el no repudio de la misma.

Por lo tanto, para conseguir una adecuada seguridad de la información hay que implementar un conjunto de controles, que incluyan políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware; además de "establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos" (ISO/IEC 27002:2005, p. 10).

De lo anterior, se infiere que un SGSI completamente seguro es aquel que se encuentra encerrado en cuarto oscuro, apagado y sin conexión a la red, por lo tanto no existe una seguridad absoluta; lo cual no implica conformarse con una cierta seguridad perimetral, pero si creer que la adopción de ciertas medidas de seguridad proporcionan la tranquilidad suficiente para que la organización se mantenga dentro de los estándares comerciales y de seguridad.

Normas que estandarizan la seguridad de la información

Existen normas que son especificaciones técnicas, de carácter voluntario, consensuadas, elaboradas con la participación de las partes interesadas (fabricantes, usuarios y consumidores, laboratorios, administración, centros de investigación) y aprobadas por un organismo reconocido. Por lo que, las normas son documentos de aplicación voluntaria y tienen el carácter de acuerdos documentados que contienen los criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características.

En el ámbito internacional ISO e IEC tienen por objetivo favorecer el desarrollo de la normalización en el mundo, para facilitar los intercambios comerciales y las

prestaciones de servicios entre los distintos países. Entre los documentos elaborados por ISO/IEC se encuentran las normas internacionales que son elaboradas por los miembros participantes en un comité técnico, subcomité o grupo de trabajo y aprobada por votación entre todos los participantes; dentro de estas normas se encuentran las que proporcionan modelos para implementar la seguridad de la información en los SGSI de las organizaciones; entre ellas se encuentran las normas ISO/IEC 27001:2005, ISO/IEC 27002:2005.

ISO/IEC 27001:2005: Tecnología de la Información - técnicas de seguridad - Sistemas de Gestión de Seguridad de la Información - Requerimientos[4]; estándar para la seguridad de la información publicado por la Organización Internacional de Estandarización (ISO) y por la Comisión Electrotécnica Internacional (IEC); tiene su origen en la norma BS[5] 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI; ha sido preparada para especificar los requisitos necesarios para "establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI" (p. 5), y adopta el modelo del "ciclo de Deming", Planear-Hacer-Chequear-Actuar[6] (PDCA), que se aplica a todos los procesos SGSI (ver figura 1); y consta de un anexo A que enumera en forma de resumen los objetivos de control y los controles que desarrolla la norma ISO/IEC 27002:2005.

En otras palabras, es el conjunto de especificaciones contra la cual las organizaciones pueden solicitar la certificación de sus SGSI. Este estándar internacional se alinea con el ISO 9001:2000 e ISO 14001:2004 para dar soporte a una implementación y operación consistente e integrada con los estándares de gestión relacionados.

[4] Original en ingles: Information technology – Security techniques – Information security management systems – Requirements.
[5] BS: British Standards
[6] Original en ingles: Plan, Do, Check, Act

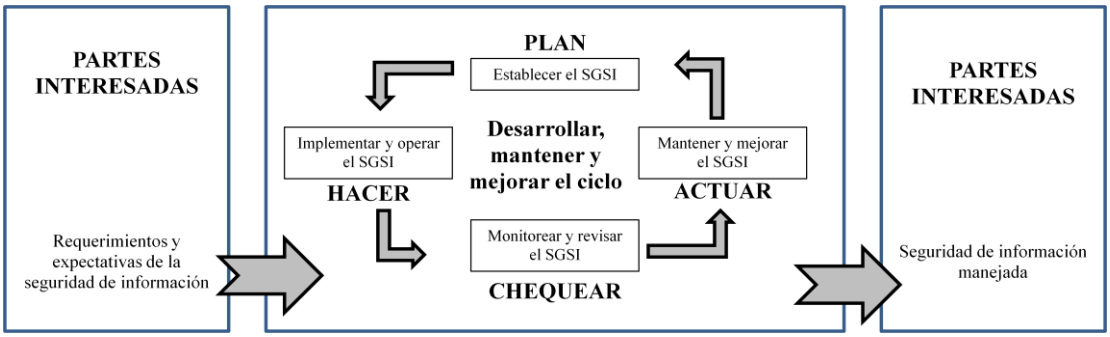


Figura 1: Modelo PDCA aplicado a los procesos SGSI
Fuente: ISO/IEC 27001:2005

ISO/IEC 27002:2005: antigua ISO/IEC 17799:2000, Tecnología de la Información - Técnicas de Seguridad – Código de buenas prácticas para la Gestión de la Seguridad de la Información[7]; estándar internacional publicado también por ISO/IEC; la cual es un instrumento para la gestión de la seguridad de la información que aporta un conjunto de 39 objetivos de control y 133 controles y de recomendaciones que se encuentran agrupados en 11 dominios; la cual tiene como objetivos principales identificar controles independientes de la tecnología, facilitar la adopción de controles proporcionados al riesgo, atender la demanda relativa al desarrollo, implantación y medida de prácticas de seguridad efectivas, proporcionar principios y recomendaciones de gestión en lo que basar la política de seguridad.

Es decir, es una guía para, en cualquier contexto, conocer qué se puede hacer para mejorar la seguridad de la información, la cual expone en distintos campos, una serie de apartados relacionados con la seguridad, los objetivos de seguridad a seguir, una serie de consideraciones para cada objetivo y un conjunto de sugerencias para cada uno de esos controles.

[7] Original en ingles: Information technology – Security techniques – Code of practice for information security management

Sistemas de Gestión de Seguridad de la Información (SGSI)

Un sistema de gestión de seguridad de la información (SGSI) es denominado por la norma ISO/IEC 27001:2005, como "esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial, para establecer, implementar, operar, revisar, mantener y mejorar la seguridad de la información" (p. 10). Por consiguiente, un SGSI comienza por su correcto diseño y para ello la norma ISO/IEC 27001:2005 indica que debe estar formado por:

a) **Alcance del sistema**, donde se determinan las partes o procesos de la organización que van a ser incluidos, decidir qué se quiere proteger y por donde debe empezar, así como también, deben quedar definidas las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedarán excluidas en la implantación del sistema y es importante que durante esta fase, se estimen los recursos económicos y de personal que se van a dedicar a implantar y mantener el sistema.
b) **Definir las políticas y objetivos de seguridad,** recoge las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y a la legislación vigente, además de establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades; así como también debe explicar que es lo que está permitido y que no; determinar los límites del comportamiento aceptable y cuál es la respuesta si esto se sobrepasan.
c) **Estándares, procedimientos y guías que soportan el SGSI,** aquellos documentos y mecanismos que regulan el propio funcionamiento del SGSI; documentación necesaria para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
d) **Metodología de análisis y evaluación de riesgos,** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información

contenidos dentro del alcance seleccionado), tratamiento y desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

e) **Informe de evaluación de riesgos (Risk Assessment),** estudio resultante de aplicar la metodología de análisis y evaluación de riesgos mencionada anteriormente, a los activos de información de la organización.
f) **Plan de tratamiento de riesgos,** documento que identifica las acciones de la alta dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
g) **Registros,** documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
h) **Declaración de aplicabilidad,** (SOA –Statement of applicability -, en sus siglas en inglés); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de análisis y evaluación de riesgos, justificando inclusiones y exclusiones.

Por lo tanto, un SGSI consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización; por lo que, su propósito no es garantizar la seguridad, sino asegurar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías. Cabe destacar, que un SGSI protege a los activos de información de una entidad, independientemente del medio en que se encuentren; por ejemplo, correos electrónicos, informes, páginas web, documentos, hojas de cálculo, presentaciones, información confidencial de sus trabajadores, etc.

En conclusión, un SGSI ayuda a las instituciones a gestionar de forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal

dirigidas que se producen para contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un costo más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada de incidencias o la continuidad de la entidad.

Análisis de riesgos

Activos

Denominados por la norma ISO/IEC 27002:2005 como "cualquier cosa que tenga valor para la organización" (p. 13); de la misma manera, la metodología MAGERIT (2006) lo define como "los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección" (p. 17). Es de acotar, que no todos los activos son de la misma especie, así dependiendo del tipo de activo, las amenazas y salvaguardas son diferentes.

En este sentido, MAGERIT (2006) indica que el activo esencial es la *información* que maneja el sistema, y alrededor de estos datos se pueden identificar otros activos relevantes como:

a) **Los servicios**, que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
b) **Aplicaciones informáticas,** que permiten manejar los datos (software).
c) **Equipos informáticos (hardware),** que permiten hospedar datos, aplicaciones y servicios.

d) **Soportes de información,** que son dispositivos de almacenamiento de datos.
e) **Equipamiento auxiliar,** que contempla el material informático.
f) **Redes de comunicación,** que permiten intercambiar datos.
g) **Instalaciones,** que acogen equipos informáticos y de comunicaciones.
h) **Personas,** que operan todos los elementos anteriores.

Por otro lado, un activo interesa por lo que vale; es decir, si algo no vale para nada prescíndase de ello y si no se puede prescindir de un activo, entonces es que algo vale y eso es lo que hay que averiguar, pues eso es lo que hay que proteger y cuando se habla de valor del activo no se está refiriendo a cuánto cuesta (MAGERIT V.2, 2006, p. 19).

Amenazas

Es definida por la ISO/IEC 27002:2005 como "una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización" (p. 16); de la misma manera y para una mejor comprensión, Stalling (2004) expone que "es una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio" (p. 5); por lo que se refiere a aquello que desencadena acontecimientos indeseados y que puede repercutir negativamente en el sistema y la organización a que pertenece.

En este sentido, la probabilidad de que una amenaza se haga realidad depende de la frecuencia de la misma, la motivación así como la capacidad y recursos con que cuenta un agresor potencial, la vulnerabilidad del sistema y sus componentes, y el valor que tenga el sistema para la organización y el agresor.

De lo anterior, se puede inferir que una amenaza son los eventos que pueden desencadenar un incidente, produciendo daños materiales o inmateriales en los activos. En este sentido, Daltabuit y otros (2007) expresan que "existen cuatro tipos de amenazas principales a los sistemas que explotan las vulnerabilidades de los activos en el sistema. Estas amenazas son: interrupción, intercepción, modificación y fabricación" (p. 93), tal como se muestran en la figura 2, donde A representa la fuente u origen de los datos, B representa al receptor o destino de ellos; tanto A como B pueden ser personas, procesos, dispositivos o computadoras (Daltabuit y otros, 2007, p. 93).

a) **Interrupción:** es cuando un activo del sistema se daña, se pierde, se destruye o llega a no estar disponible (Daltabuit y otros, 2007, p. 94), lo que hace su detección inmediata; donde el servicio de seguridad afectado es la disponibilidad. Como ejemplos se pueden citar la destrucción de un disco duro, el borrado de programas o datos, la interrupción de una línea de comunicación, etc.
b) **Intercepción**: según Daltabuit y otros (2007) significa "que alguna parte no autorizada logre acceso a un activo del sistema" (p. 94), esta parte puede ser una persona, un programa, un computador, un proceso u otro sistema de computo, también se puede decir, es cuando se hace uso de privilegios no adquiridos, por lo que su detección es difícil y a veces no deja huellas. Ésta es una amenaza al servicio de seguridad de confidencialidad. Como ejemplos de ésta se pueden citar el copiado ilícito de programas o archivos, las intervenciones de las líneas para capturar datos.
c) **Modificación**: "cuando una parte no autorizada logra el acceso al activo del sistema y puede manipular ese activo" (Daltabuit y otros, 2007, p. 95), es decir, es el acceso no autorizado que cambia la información para su beneficio deteriorando el activo, siendo ésta una agresión a la integridad y su detección es difícil según las circunstancias. Algunos ejemplos, son los cambios de valores en un fichero de datos, la alteración de un programa para que funcione de una forma diferente, la modificación del contenido de los mensajes que se transmiten en una red, las modificaciones de bases de datos.

d) **Fabricación**: "una parte no autorizada puede fabricar objetos falsos en un sistema" (Daltabuit y otros, 2007, p. 95); es decir, se crean o insertan nuevos objetos dentro del sistema, siendo ésta una agresión a la autenticidad. Algunos ejemplos son la incorporación de registros a un fichero, la introducción de mensajes falsos a una red, etc.

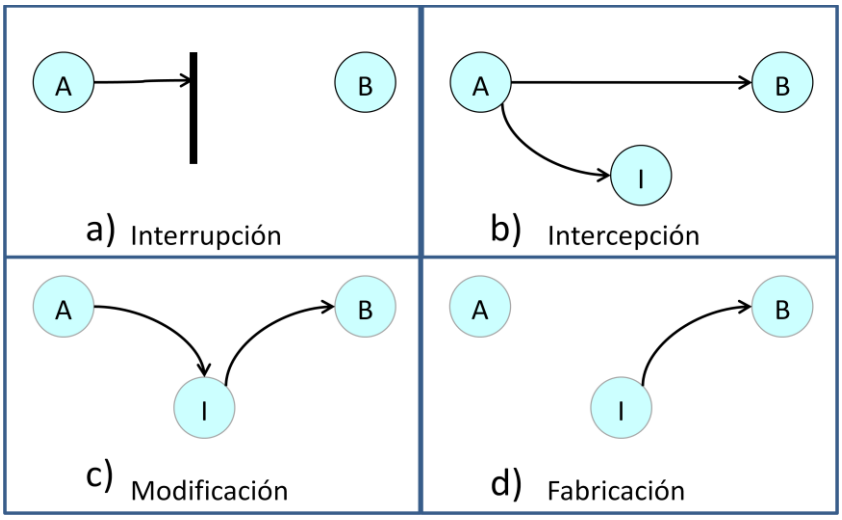


Figura 2: Tipos de amenazas
Fuente: Autor (2010)

Por otro lado, Daltabuit y otros (2007) indican que un ataque se define como "cualquier acción que explota una vulnerabilidad" (p. 96), los cuales se clasifican de manera general en activos y pasivos.

En los ataques pasivos el atacante no altera, modifica información, sino que únicamente la escucha o monitorea con el fin de obtener información que está siendo transmitida y tiene por objetivos interceptar datos y analizar tráfico; es decir, consiste sólo en observar comportamientos o leer información, sin alterar ni el estado del sistema ni la información (Daltabuit y otros (ob. cit.), p. 96).

Mientras que, los ataques activos "tienen la capacidad de modificar o afectar la información o el estado del sistema o a ambos" (Daltabuit y otros, 2007, p. 96); es decir, el atacante si modifica el flujo de datos o implican la creación de falsos flujos

de datos, generalmente son realizados por hackers, piratas informáticos, entre otros. Dentro de este tipo encontramos el enmascaramiento, la repetición, modificación de mensajes y la denegación del servicio (DoS).

Vulnerabilidad

En la norma ISO/IEC 27002:2005, se expresa que es "la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas" (p. 16); por otro lado, Daltabuit y otros (2007) la definen como "cualquier debilidad que puede explotarse para causar pérdida o daño al sistema… el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema" (p. 93). En otras palabras, es toda aquella característica de un activo que permite la consecución de ataques que comprometen la confidencialidad, integridad, disponibilidad y el no repudio de los activos de una organización.

Riesgo

La seguridad de la información contempla un elemento fundamental como lo es el análisis de riesgo, que se encarga de detectar las debilidades y de buscar un remedio para ellas. En este sentido, Carracedo (2004) define riesgo como la "posibilidad (la probabilidad) de que se produzca un impacto dado en un activo, es decir, que un agente amenazante explote una vulnerabilidad y provoque un efecto negativo en el sistema" (p. 37). Al igual que, la norma ISO/IEC 27005:2008 que sirve como guía para la gestión de riesgos de la seguridad de la información en los SGSI expresa, que riesgo de seguridad de la información es el "potencial de que una amenaza explote las vulnerabilidades de un activo o grupo de activos causando daño a la organización" (p. 1).

De esta manera, a las definiciones anteriores se les denomina *"riesgo basado en amenazas, vinculado o no a vulnerabilidades"*, a partir de la cual, se puede concluir que riesgo es la combinación de un activo, una amenaza capaz de dañar ese activo y las vulnerabilidades explotadas por la amenaza para dañar dicho activo.

Es de hacer notar que el modelo de riesgo basado en amenazas/vulnerabilidades es un *"modelo de riesgo estático"* en el que los elementos bajo consideración no incorporan al tiempo como variable y es imposible describir las secuencias de eventos, causas o consecuencias.

Por otro lado, la norma ISO/IEC 27002:2005 expresa otra definición de riesgo como "la combinación de la probabilidad de un evento y sus consecuencias" (p. 14); llamándose esta "*riesgo basado en escenarios o riesgo basado en situaciones"*, deduciendo de esta manera que riesgo es la combinación de un elemento activo, un tipo de daño que puede ocurrirle al activo y las circunstancias en que estos daños pueden ocurrir. Así, una circunstancia puede ser descrita como:

a) Una amenaza genérica que describe una tipología de circunstancias, y
b) Circunstancias específicas que identifican una amenaza genérica.

Cabe destacar, que el modelo de riesgo basado en escenarios es un *"modelo de riesgo dinámico*", en el cual el tiempo juega un rol y como resultado, diferentes fases del escenario del riesgo en cuestión resultan en diferentes tipos de acción.

Análisis de riesgos

Martínez (2002), define al análisis de riesgos como una:

> Poderosa herramienta que permite establecer un marco sistemático que provee los indicadores adecuados para llevar acciones de control, mitigación o eliminación de peligros, riesgos e impactos adversos o no deseados en el transcurso de nuestras actividades, cualesquiera que estas sean (p. 44).

Es importante considerar el análisis de riesgo como el núcleo de toda organización en cuanto a la seguridad de la información, porque permite establecer un nivel adecuado de seguridad que se aspira lograr en la protección de los activos, de qué o quién protegerlos y cómo hacerlo, teniendo como guía la normativa ISO 27005:2008, que establece criterios sobre la gestión del riesgo proporcionando un marco normalizado para definir metodologías propias de análisis de riesgo, la normativa ISO 27002:2005 que facilita la adopción de controles proporcionados al riesgo y la norma ISO/IEC 27001:2005 que proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI. Por lo tanto, el análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos.

Es lógico entender entonces, según expone Martínez que el análisis de riesgos es "perfectible, por lo que siempre tendrá ventajas, desventajas y diferentes objetivos de acuerdo al entorno y punto de vista de la institución, empresa o comunidad en la cual se aplique" (p. 44).

En este sentido, el análisis de riesgo comprende las vulnerabilidades y las amenazas y es un elemento fundamental para determinar las medidas de seguridad de un activo, sistema, o lo que se esté analizando, ya que identifica los riesgos y estima el impacto potencial que supone la pérdida de disponibilidad, confidencialidad e integridad de la información, esto en concordancia con lo planteado por Royal (1998), quien expresa que:

> No todas las exposiciones necesitan ser o deberían ser controladas, el control total no es un costo eficaz y generalmente es muy ineficiente, sin embargo, si el diseñador no tiene idea de que la exposición presenta el mayor riesgo en términos de frecuencia de ocurrencia y costo, no tiene otra alternativa que controlar cada exposición (p. 83).

De lo expuesto anteriormente, se deduce que el análisis de riesgo debe ser coordinado dentro de una estrategia bien definida para obtener como resultados, la consolidación de las vulnerabilidades para identificar los pasos a seguir para su corrección, la identificación de las amenazas que pueden explotar esas vulnerabilidades y así llegar a su corrección o mitigación, la identificación de los

impactos potenciales que pudieran tener los incidentes y de esta forma aprovechar las vulnerabilidades encontradas, y la determinación de las recomendaciones para que las amenazas sean corregidas o reducidas; todo esto para mejorar la seguridad así como la sensibilización del personal de la organización.

Norma ISO/IEC 27005:2008 - Information technology - security techniques - information security risk management

Esta norma sirve como guía para la gestión de riesgos de seguridad de la información, de acuerdo con los principios definidos en las otras normas de la serie 27000, sustituye y actualiza a la norma ISO/IEC TR 13335-3:1998 y a la norma ISO/IEC 13335-4:2000 (Técnicas para la gestión de la seguridad IT y selección de salvaguardas, respectivamente), según lo expone la misma norma ISO/IEC 27005:2008. Por lo que, se convierte en la principal guía para el desarrollo de las actividades de análisis y tratamiento de riesgos en un SGSI, además constituye una ampliación del apartado 4.2.1 de la norma ISO/IEC 27001 en donde se presenta el análisis de riesgos.

Por consiguiente, esta norma *no ofrece ninguna metodología específica* para la gestión de los riesgos, sino que corresponde a cada organización definir su propio enfoque de gestión de riesgos dependiendo, por ejemplo, del alcance del SGSI, el contexto o del sector industrial; de igual manera, soporta los conceptos especificados en la norma ISO/IEC 27001 y está diseñada para contribuir a la aplicación satisfactoria de seguridad de la información basado en el enfoque de gestión de riesgos, y es aplicable a todo tipo de organizaciones (ISO/IEC 27005:2008).

En este sentido, el estándar ISO/IEC 27005 expresa que la gestión de riesgos de seguridad de la información debe ser una parte integral de todas las actividades de gestión de seguridad de la información y se debe aplicar tanto a la implementación y la operación continua de un SGSI. Por otro lado, en este estándar se manejan las dos

definiciones de riesgo: *basado en amenazas/vulnerabilidades* y *basado en escenarios de riesgo.*

Igualmente, contiene la descripción del proceso de seguridad de la información de gestión de riesgos y sus actividades y está estructurada de la siguiente manera:

Clausula 5: Antecedentes

Clausula 6: Visión general del proceso de gestión de riesgos, y sus actividades.

Donde, el proceso de gestión de riesgos se describe a partir de la siguiente clausula:

Clausula 7: Estableciendo el contexto, se definen los objetivos, el alcance y la organización para todo el proceso.

Clausula 8: Evaluación de riesgos, en la que se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Está dividida en tres (3) apartados:

1) **Clausula 8.1: Descripción general de la evaluación de riesgos de seguridad de la información.**
2) **Clausula 8.2: Análisis de riesgos**
   - ✓ **Clausula 8.2.1: Identificación de riesgos**, consiste en determinar qué puede provocar pérdidas a la Organización.
     - o **Clausula 8.2.1.1:** Introducción a la identificación de riesgos.
     - o **Clausula 8.2.1.2:** Identificación de activos.
     - o **Clausula 8.2.1.3:** Identificación de amenazas.
     - o **Clausula 8.2.1.4:** Identificación de controles existentes.
     - o **Clausula 8.2.1.5:** Identificación de vulnerabilidades
     - o **Clausula 8.2.1.6:** Identificación de consecuencias.
   - ✓ **Clausula 8.2.2: Estimación de riesgos**, consiste en usar métodos cuantitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta los activos, las amenazas y las salvaguardas.
     - o **Clausula 8.2.2.1:** Metodologías para estimar el riesgo

- **Clausula 8.2.2.2:** Valoración de las consecuencias.
- **Clausula 8.2.2.3:** Valoración de la probabilidad del incidente.
- **Clausula 8.2.2.4:** Estimación del nivel de riesgo

3) **Clausula 8.3: Evaluación de riesgos:** consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

Clausula 9: Tratamiento de riesgos, en esta clausula se define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.

Clausula 10: Aceptación de riesgos, aquí se determinan los riesgos que se deciden aceptar y la justificación correspondiente de cada riesgo aceptado.

Clausula 11: Comunicación de riesgos, en la que todos los grupos de interés intercambian información sobre los riesgos.

Clausula 12: Monitoreo y revisión de riesgos, donde el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos.

Anexo A: Definición del alcance y límites del proceso de la gestión de riesgos

Anexo B: Identificación y valoración de los activos y evaluación del impacto

Anexo C: Ejemplos de Amenazas típicas

Anexo D: Ejemplos de vulnerabilidades típicas

Anexo E: Ejemplos de enfoques de evaluación de riesgos

Anexo F: Restricciones para la reducción de riesgos

A continuación, se presenta de forma gráfica el proceso de gestión de riesgos definido por este estándar:

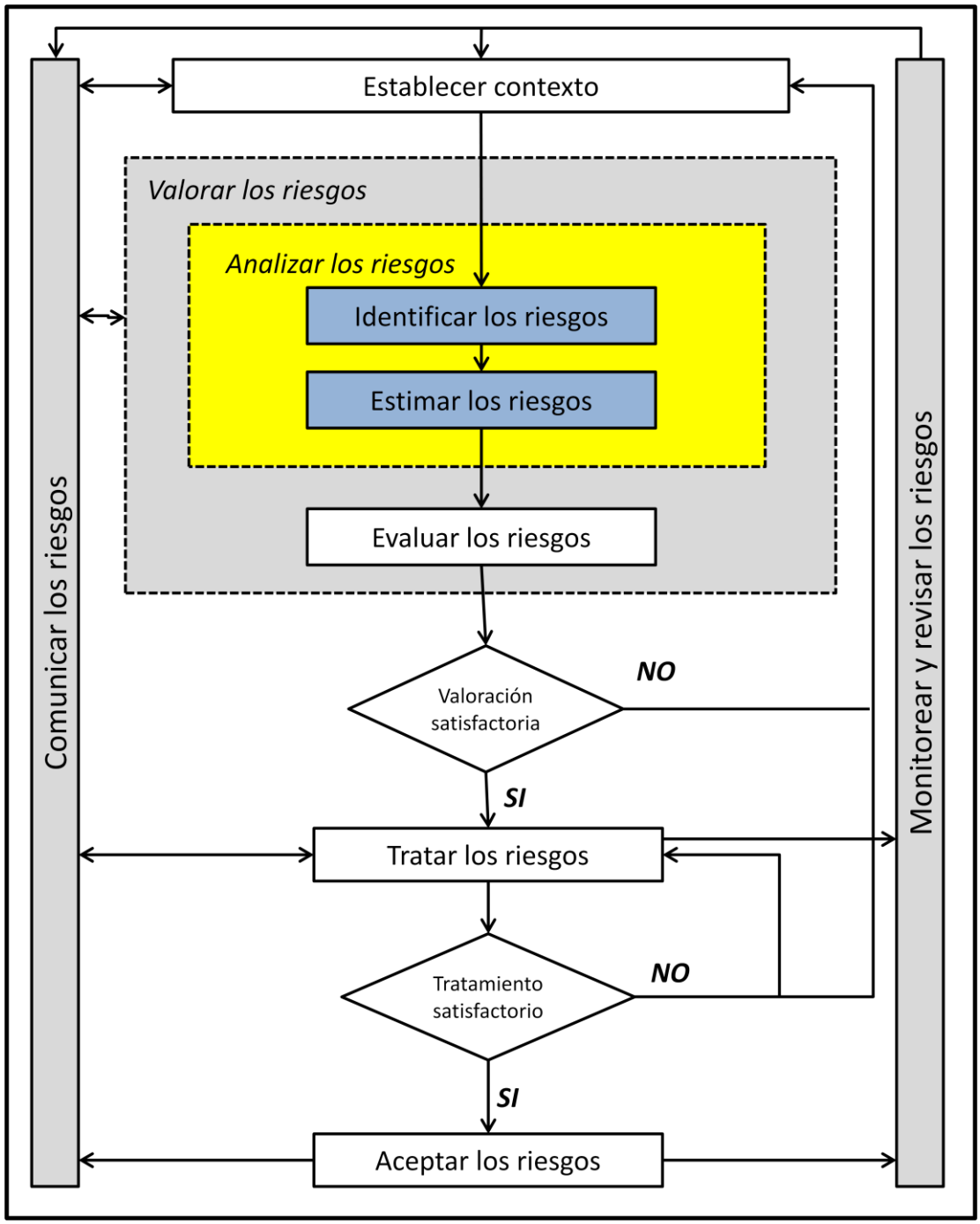


Figura 3: Proceso de gestión de riesgos de seguridad de la información de ISO/IEC 27005:2008
Fuente: ISO/IEC 27005:2008

Metodologías para el análisis de riesgos

Existe una gran variedad de metodologías que se encargan del análisis y gestión de riesgos a los SGSI a nivel mundial, muchas de ellas con reconocimiento internacional, pero lamentablemente todas distintas. Es cierto que, como metodologías de análisis de riesgos que son, todas se parecen, pero no se puede decir que sean compatibles. Cada una tiene sus particularidades, sus puntos fuertes y débiles, y queda a criterio de quien desee usarlas sacar lo mejor de cada una de ellas para elaborar una que se amolde a la organización.

Con referencia a lo anterior, existen metodologías que realizan los procesos de análisis y gestión del riesgo tomando en cuenta las 2 definiciones de riesgos existentes: basado en amenazas/vulnerabilidades y basado en escenarios; es allí donde radica la diferencia de estas metodologías.

Por lo que, en la presente investigación se estudiaron y se realizó un análisis comparativo entre ellas para obtener los criterios que permitieron diseñar una metodología acorde a las necesidades de las instituciones universitarias en estudio; entre ellas están: MAGERIT, CRAMM, OCTAVE, EBIOS y MEHARI. A continuación, se presenta una descripción detallada de cada una de las metodologías mencionadas:

MAGERIT, es una metodología abierta de análisis y gestión de riesgo para los sistemas de información, elaborada por el Consejo Superior de Administración Electrónica (CSAE) y publicada por el Ministerio de Administraciones Pública, para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, basada en la Administración Pública. Recomienda las medidas apropiadas que deberían adoptarse para *conocer, prevenir, impedir, reducir o controlar* los riesgos investigados; así MAGERIT V.2. (2006) expone que la razón de ser está "directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los

ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza" (p. 6).

Adicionalmente, la primera versión de la metodología MAGERIT se publicó en el año de 1.997 y la versión vigente es la 2.0 publicada en el año 2.006, la cual dispone de una herramienta de soporte llamada PILAR II (Proceso Informático-Lógico para el Análisis y Gestión de riesgo), es de uso gratuito para la administración pública Española y de uso comercial para las organizaciones privadas.

Cabe agregar que, MAGERIT V.2 está estructurada en tres libros diferenciados:

Libro I – Método: volumen principal que describe la metodología desde 3 ángulos:

a) **El capitulo 2:** describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación y es una presentación netamente conceptual.
b) **El capítulo 3:** describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente pautar roles, actividades, hitos y documentación para que la realización del proyecto esté bajo control en todo momento.
c) **El capítulo 4:** aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento de los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento.
d) **El capítulo 5:** desgrana una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo para la realización de un análisis de riesgos y una gestión totalmente efectivo.
e) **Los apéndices:** recogen material de consulta como: glosario, referencias bibliográficas, referencias al marco legal, el marco normativo de evaluación y certificación, las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos.

Libro II - Catálogo de elementos: en libro aparte, se propone un catálogo abierto de ampliaciones que marca pautas en cuanto a:

- ✓ Tipos de activos.
- ✓ Dimensiones y criterios de valoración.
- ✓ Amenazas típicas sobre los sistemas de información.
- ✓ Salvaguardas a considerar para proteger sistemas de información.

Además, se persigue por un lado, facilitar la labor de las personas que acometen el proyecto, ofreciéndoles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto de estudio y por otro lado, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Libro III - Guía de técnicas: complementa el libro I proporcionando una introducción de algunas técnicas a utilizar en las distintas fases del análisis de riesgo; las técnicas que recoge son:

- ✓ Técnicas específicas para el análisis de riesgo
  - Análisis mediante tablas
  - Análisis algorítmico
  - Arboles de ataque
- ✓ Técnicas generales
  - Análisis costo-beneficio
  - Diagramas de flujo de datos
  - Diagramas de procesos
  - Técnicas gráficas
  - Planificación de proyectos
  - Sesiones de trabajo: entrevistas, reuniones y presentaciones
  - Valoración Delphi

Sobre la base de las consideraciones anteriores, MAGERIT es compatible con las normas ISO/IEC 27001, 15408, 17799 y 13335 y persigue los siguientes objetivos: Concienciar a los responsables de los Sistemas de Información de la existencia de riesgos y de la necesidad de detectarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las salvaguardas oportunas para mantener los riesgos bajo control, apoyar a la Organización en la preparación de los procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso (MAGERIT V.2., 2006, p. 6).

Finalmente, se puede resumir gráficamente el proceso del modelo de la metodología MAGERIT como muestra la figura 4:

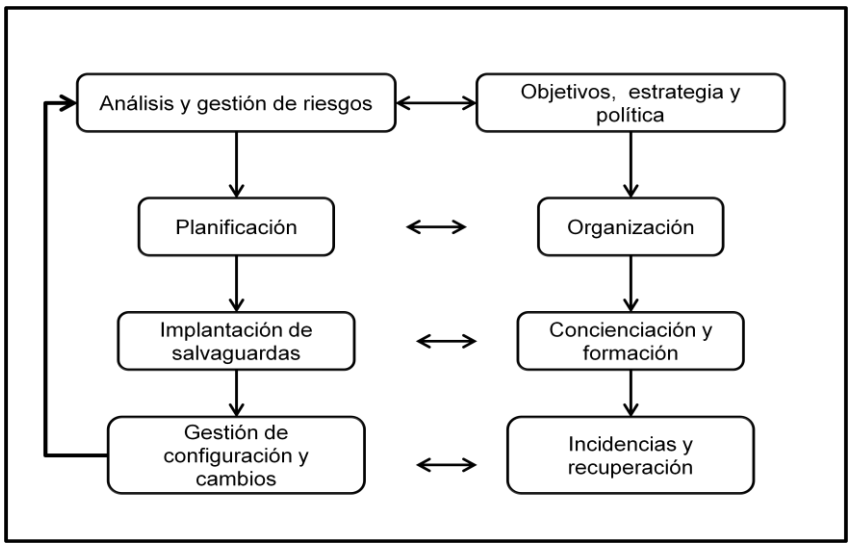


Figura 4: Metodología MAGERTI
Fuente: MAGERIT

MAGERIT V.2 realiza el proceso de análisis de riesgos usando la definición de riesgo basado en amenazas/vulnerabilidades; a través de unos pasos pautados a saber y son representados gráficamente en la figura 5:

a) Determinar los activos relevantes, su interrelación y su valor.
b) Determinar a qué amenazas están expuestos esos activos.
c) Determinar qué salvaguardas hay dispuestas

d) Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
e) Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

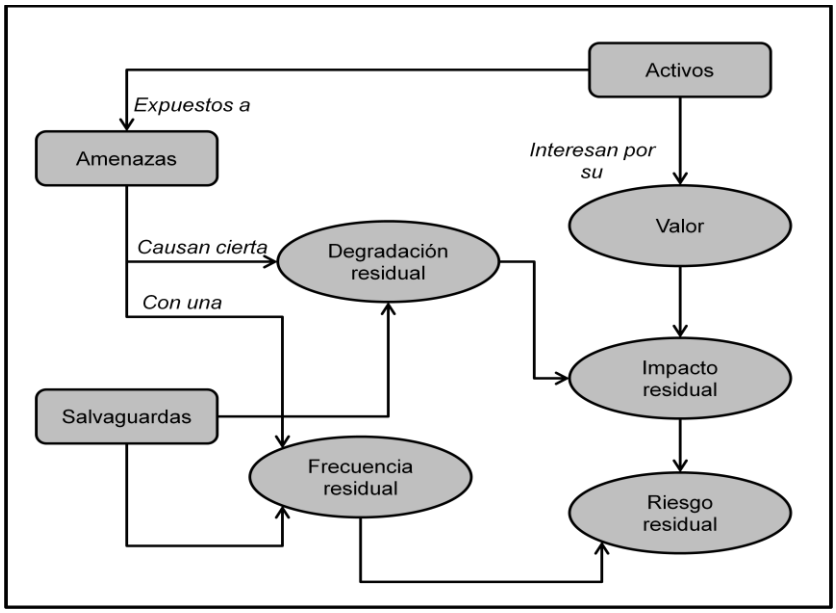


Figura 5: Análisis de riesgos de la Metodología MAGERTI
Fuente: MAGERIT

CRAMM – Computer Risk Analysis and management method (Método de análisis y gestión de riesgos de computadores); metodología que utiliza técnicas cualitativas para el análisis de riesgos desarrollada por la Organización Británica CCTA - Central Communication and Telecommunication Agency -, creada en 1987 y actualmente utilizada por la OTAN, ejército de Holanda, Unisys y numerosas corporaciones en todo el mundo que trabajan activamente en seguridad; a pesar de tratarse de una iniciativa del sector público, el mantenimiento y la gestión de la metodología lo realiza una empresa privada de consultoría: Insight Consulting.

En igual forma, la metodología CRAMM comprende tres fases para la realización del análisis de riesgo:

- ✓ **Fase I: Establecimiento de objetivos de seguridad:**
  - Definir el alcance del estudio.
  - Definir el valor de la información entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación.
  - Identificar y evaluar los activos físicos que forman parte del sistema.
  - Identificar y evaluar los activos de software que forman parte del sistema.
- ✓ **Fase II: Análisis de riesgo:**
  - Identificar y valorar el tipo y el nivel de las amenazas que pueden afectar al sistema.
  - Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas.
  - Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.
- ✓ **Fase III:** Identificación y selección de salvaguardas.

Adicionalmente, como característica más resaltante esta su compatibilidad con las normas ISO/IEC 17799 y 27001, también usa una herramienta llamada CRAMM como apoyo, la cual proporciona un soporte con una base de datos de:

- ✓ Más de 400 tipos de activos.
- ✓ Más de 25 tipos de impacto.
- ✓ Más de 38 tipos de amenazas.
- ✓ 7 tipos de medidas del riesgo.
- ✓ Más de 3.500 salvaguardas.

Así mismo, en la actualidad CRAMM soporta dos tipos de revisiones: CRAMM Experts y CRAMM express.

En este sentido, el proceso del modelo de análisis y gestión de riesgo de CRAMM es basado usando la definición de riesgo basado en amenazas/vulnerabilidades, tal como lo indica la figura 5:

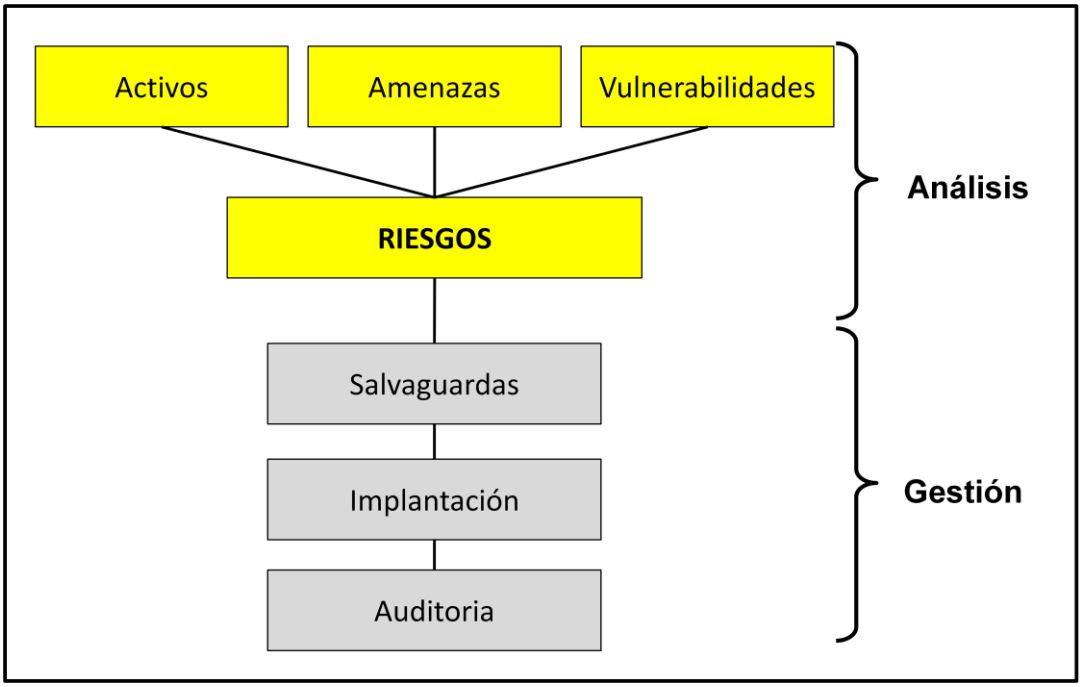


Figura 6: Fases del proceso de la Metodología CRAMM
Fuente: Análisis de riesgos de seguridad de la información (2009)

Por otra parte, los principales productos de la metodología CRAMM son los siguientes:

- ✓ Documento de inicio del proyecto.
- ✓ Informes de análisis de riesgo.
- ✓ Informes de gestión de riesgo, basados en una base de datos de más de 3.500 salvaguardas técnicas y organizativas.
- ✓ Plan de implantación.

En síntesis, se resume las principales actividades del proceso de análisis y gestión de riesgo de la metodología CRAMM de la siguiente manera gráfica:

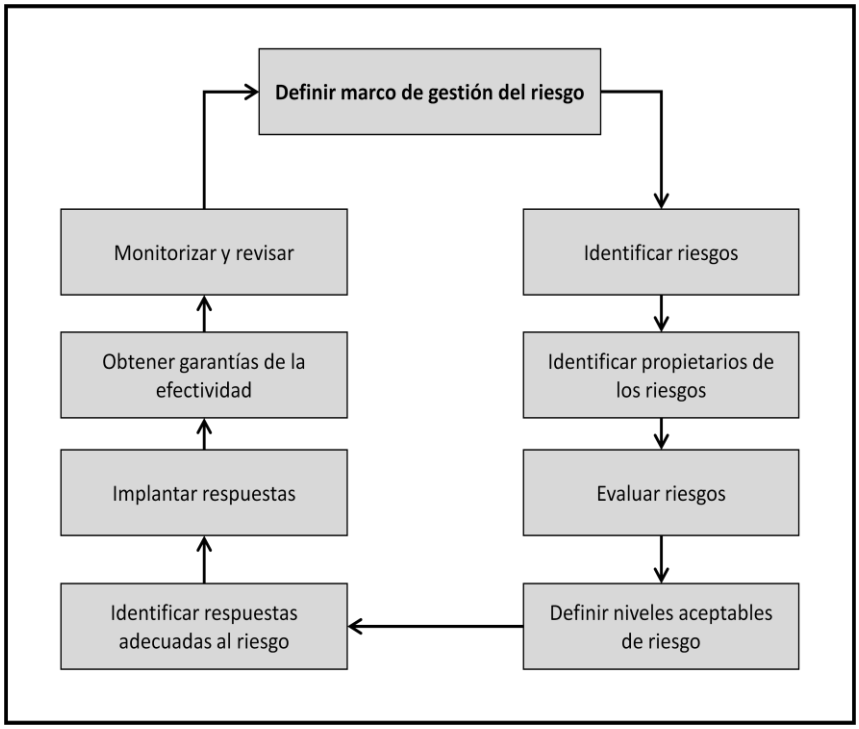


Figura 7: Actividades del proceso de análisis y gestión de riesgo de CRAMM
Fuente: Análisis de riesgos de seguridad de la información (2009)

OCTAVE, (Operationally Critical Threat, Asset, and Vulnerability Evaluation), es una metodología de evaluación de riesgo orientada a activos (definición de riesgo basado en amenazas/vulnerabilidades), desarrollada por el Instituto de Ingeniería de Software de la universidad de Carnegie Mellon que se enfoca en la estimación estratégica y en la planeación técnica de la seguridad basada en el riesgo, es auto dirigida, es decir, la misma organización se responsabiliza por la configuración de las estrategias de seguridad.

Cabe agregar, que el núcleo central de OCTAVE es un conjunto de criterios (principios, atributos y resultados) a partir de los cuales se pueden desarrollar diversas

metodologías, por lo que, cualquier metodología que aplique los criterios es considerada compatible con el modelo OCTAVE.

Actualmente, las tres (3) metodologías publicadas por el Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon son:

1) **OCTAVE:** Method Implementation Guide, es la metodología original definida para grandes organizaciones.
2) **OCTAVE-S:** Implementation Guide, Metodología disponible para las pequeñas organizaciones.
3) **OCTAVE Allegro:** Guidebook, metodología definida para analizar riesgos con un mayor enfoque en los activos de información, en oposición al enfoque en los recursos de información.

Cabe destacar que, la metodología OCTAVE usa como herramienta de apoyo *Octave Automated Tool.* En síntesis, las fases de la metodología OCTAVE se resumen de manera gráfica como lo muestra la siguiente figura:

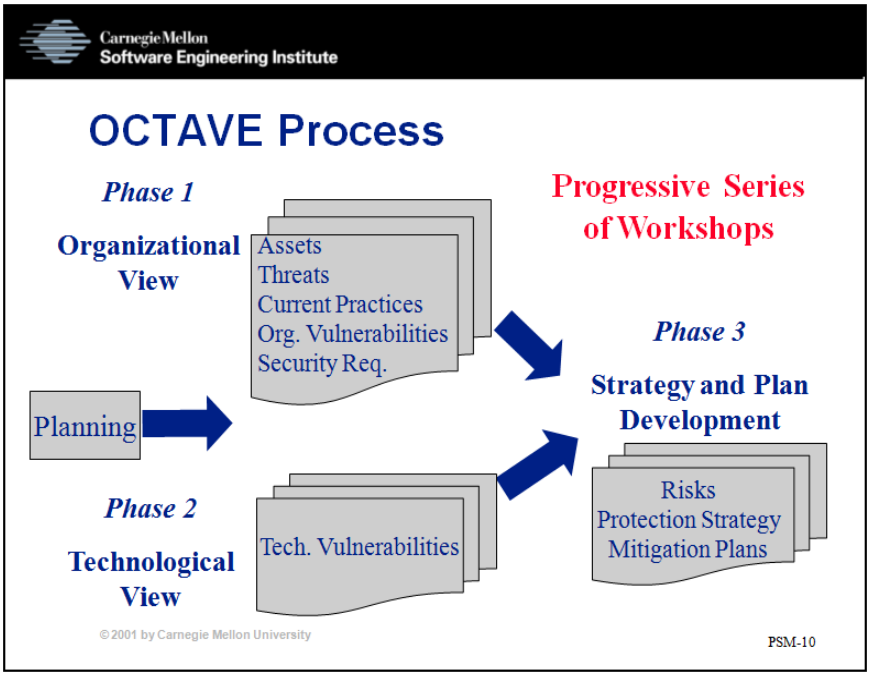


Figura 8: Fases del proceso de la Metodología OCTAVE
Fuente: OCTAVE Method Implementation Guide Version 2 (2001)

Entre los objetivos de la metodología OCTAVE se encuentran:

- ✓ Ayudar a las organizaciones a mejorar su capacidad para gestionar sus riesgos de seguridad de la información.
- ✓ Dirigir y gestionar las evaluaciones de riesgos por sí mismos.
- ✓ Tomar las mejores decisiones en función de sus riesgos particulares.
- ✓ Centrarse en la protección de los activos de información clave.
- ✓ Comunicar eficazmente información clave de seguridad

Con referencia a lo anterior, cada una de las metodologías OCTAVE define un conjunto de procesos diferentes que son:

OCTAVE:

- ✓ **Fase 1: Visión organizativa:** construcción de activos basados en perfiles de amenazas
  - Identificar conocimiento de la alta dirección
  - Identificar conocimiento de la dirección de áreas operativas
  - Identificar conocimiento del personal de áreas operativas y de TI
  - Activos
  - Crear perfiles de amenazas
  - Prácticas actúales
  - Vulnerabilidades organizacionales
  - Requerimientos de seguridad
- ✓ **Fase 2: Visión tecnológica:** identificar vulnerabilidades tecnológicas.
  - Identificar componentes claves
  - Evaluar componentes seleccionados
- ✓ **Fase 3: Desarrollo de la estrategia y del plan:** desarrollar planes y estrategias de seguridad.
  - Analizar los riesgos
  - Diseñar estrategias de protección.

OCTAVE-S

- **Fase 1: Visión organizativa**
  - Identificar información organizativa
  - Crear perfiles de amenazas
- **Fase 2: Visión tecnológica**
  - Examinar la infraestructura tecnológica relacionada con los activos críticos.
- **Fase 3: Estrategia y desarrollo del plan**
  - Analizar los riesgos
  - Diseñar la estrategia de protección y planes de mitigación

OCTAVE Allegro

- ✓ **Fase 1: Establecer dirección**
  - Establecer criterios de valoración de riesgos
- ✓ **Fase 2: Perfilar activos**
  - Desarrollar perfiles de activos de información
  - Identificar recursos de información
- ✓ **Fase 3: Identificar amenazas**
  - Identificar áreas de interés para el análisis
  - Identificar escenarios de amenazas
- ✓ **Fase 4: Identificar y mitigar riesgos**
  - Identificar riesgos
  - Analizar riesgos
  - Seleccionar enfoque de mitigación

En igual forma, los criterios que forman el núcleo de la metodología OCTAVE se mencionan a continuación:

a) Principios de los que se derivan atributos:

- ✓ La metodología debe ser auto-dirigida
  - Equipo de análisis
  - Capacidades del equipo de análisis

- ✓ Las medidas deben ser adaptables a las necesidades
  - Catalogo de practicas
  - Perfil genérico de amenazas
  - Catálogo de vulnerabilidades
- ✓ El proceso debe ser definido
  - Actividades de evaluación definidas
  - Documentación de los resultados de la evaluación
  - Alcance de la evaluación
- ✓ El proceso debe ser continuo
  - Próximos pasos
  - Catálogo de prácticas
- ✓ El proceso debe seguirse con visión de futuro
  - Enfoque de riesgos
- ✓ El proceso debe centrarse en un reducido número de riesgos críticos
  - Alcance de la evaluación
  - Actividades enfocadas
- ✓ Gestión integrada
  - Aspectos organizativos y tecnológicos
  - Participación de negocio y de áreas tecnológicas
  - Participación de la alta dirección
- ✓ Comunicación abierta
  - Enfoque colaborativo
- ✓ Perspectiva global
  - Aspectos organizativos y tecnológicos
  - Participación de negocio y de áreas tecnológicas
- ✓ Enfoque de trabajo
  - Equipo de análisis
  - Capacidades del equipo de análisis
  - Participación de negocio y de áreas tecnológicas
  - Enfoque colaborativo

b) Resultados de las distintas fases:

- ✓ Fase 1: Visión organizativa
  - Activos críticos
  - Requerimientos de seguridad para los activos críticos
  - Amenazas sobre los activos críticos
  - Prácticas de seguridad actuales
  - Vulnerabilidades organizativas actuales
- ✓ Fase 2: Visión tecnológica
  - Componentes claves
  - Vulnerabilidades tecnológicas actuales
- ✓ Fase 3: Estrategia y desarrollo del plan
  - Riesgos sobre activos críticos
  - Medidas contra los riesgos
  - Estrategia de protección
  - Planes de mitigación del riesgo

MEHARI, es una metodología desarrollada por el Club Francés de la Seguridad de la Información (Clusif), se diseñó inicialmente y se actualiza continuamente, para ayudar a la CISO (Chief Information Security Officers) en la gestión de las actividades de la seguridad de la información. Donde, su objetivo primordial es "proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IEC 27005:2008, proporcionando el conjunto de herramientas y elementos necesarios para su implementación" (MEHARI, 2010, p. 3).

Adicionalmente, MEHARI presenta otros objetivos como son: a) permitir un análisis directo e individual de situaciones de riesgos descritas en los escenarios y b) proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, medio y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones consideradas.

En este sentido, se puede inferir que MEHARI es una metodología que ha sido diseñada para realizar un análisis preciso de situaciones de riesgo usando la definición basado en escenarios. Cabe acotar, que MEHARI existe desde hace 17 años proporcionando un enfoque estructurado para la evaluación del riesgo basándose en unos simples principios a saber:

a) Factores estructurales (u organizacionales), los cuales no dependen de medidas de seguridad, sino de la actividad principal de la organización, su entorno y su contexto.
b) Factores de reducción del riesgo, que son una función directa de las medidas de seguridad implantadas.

En el mismo orden de ideas, MEHARI provee un modelo de Gestión de Riesgos con componentes y procesos modulares y establece fases como la identificación, análisis, evaluación, estimación, tratamiento, aceptación y comunicación de riesgos, usando como herramienta de apoyo, RISICARE. Así, esta metodología se compone de los siguientes documentos tal y como lo expone MEHARI (2010):

a) MEHARI: conceptos y especificaciones funcionales,
b) Guías MEHARI: para:
    i. Análisis y clasificación de amenazas,
    ii. Evaluación de servicios de seguridad y
    iii. Análisis de riesgos,
c) MEHARI manual de referencia de servicios de seguridad,
d) MEHARI base de datos de conocimientos.

Con referencia a lo anterior, MEHARI es un conjunto de herramientas y funcionalidades metodológicas para la gestión de la seguridad y de las medidas asociadas, basado en un análisis de riesgos preciso (MEHARI, 2010, p. 12). Los aspectos fundamentales de esta son:

a) Su modelo de riesgos (cualitativo y cuantitativo)
b) El examen de la eficacia de las medidas de seguridad en vigor o previstas,

c) La capacidad para evaluar y simular los niveles de riesgo derivados de medidas adicionales,

d) Complementos obligatorios a los requerimientos de la norma ISO/IEC 27000 y particularmente la ISO/IEC 27005:2008.

A continuación, se presenta el proceso de análisis de riesgos que provee MEHARI.

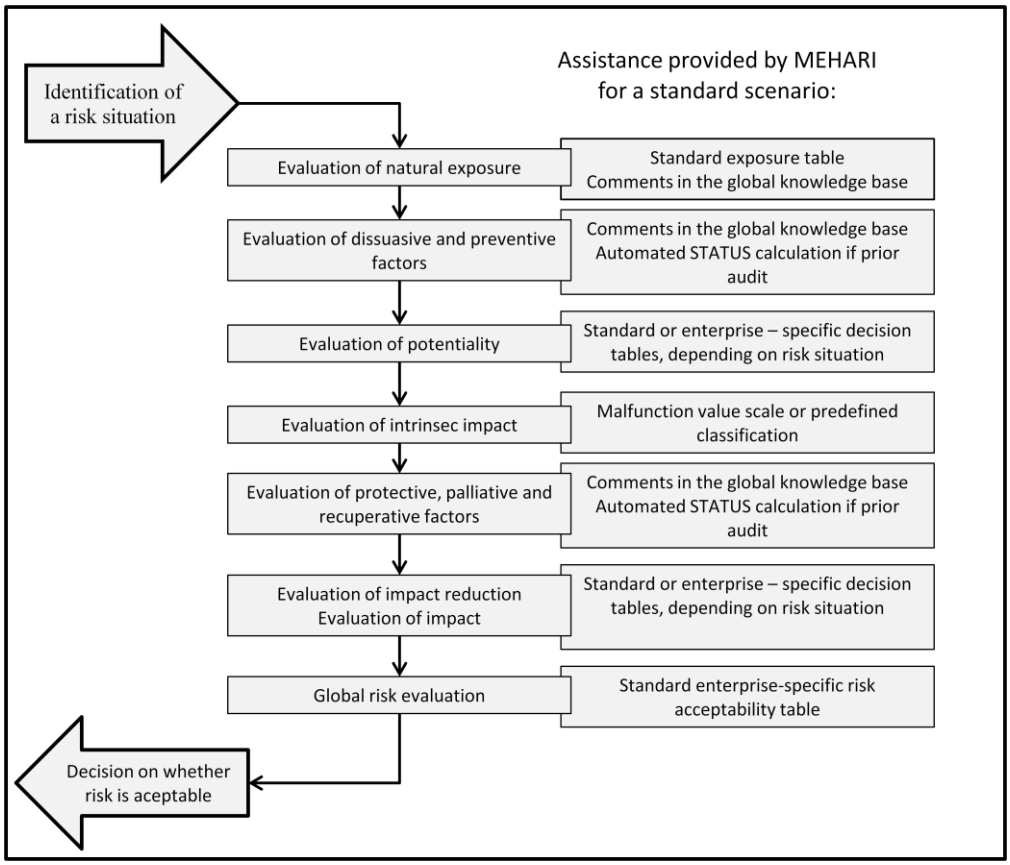


Figura 9: Proceso de análisis de riesgos de MEHARI
Fuente: MEHARI Risk Analysis Guide (2007)

Por otro lado, el proceso de identificación de situaciones de riesgos usando la base de conocimientos está basado en la selección de un conjunto de escenarios que

son específicos de la organización que se estudia y se muestra gráficamente en la siguiente figura:

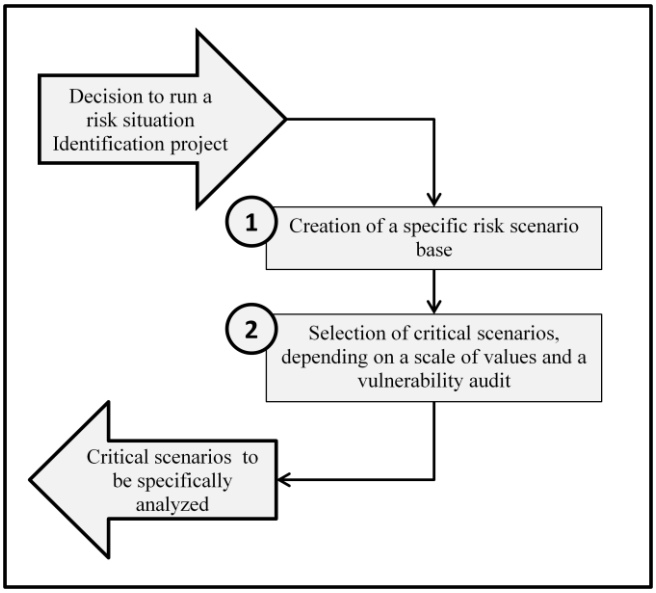


Figura 10: Identificación de situaciones de riesgos de MEHARI
Fuente: MEHARI Risk Analysis Guide (2007)

EBIOS, *(Expression des Besoins et Identification des Objectifs de Sécurite*, traducida como: *Expresión de necesidades e identificación de objetivos de seguridad.* Creada en 1995, desarrollada y mantenida por la "*Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI)*" francesa. La cual es un método que permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información, posibilita también la comunicación dentro del organismo y también con los asociados para contribuir al proceso de la gestión de los riesgos de los sistemas de información; brindando las justificaciones necesarias para la toma de decisiones (descripciones precisas, retos estratégicos, riesgos detallados con su impacto en el organismo, objetivos y requerimientos de seguridad explícitos), siendo una herramienta de negociación y arbitraje (EBIOS Méthode de gestion des risqué, 2010, p. 12).

Además, es ampliamente usada en el sector público (la totalidad de los ministerios y de los organismos bajo la tutela estatal), en el sector privado (gestorías, pequeñas y grandes empresas) en Francia y en el extranjero (Unión Europea, Quebec, Bélgica, Túnez, Luxemburgo, etc.), proporcionando un manejo de riesgo de alto nivel y permitiendo tener una visión global y coherente, apoyando la alta gerencia. Cabe destacar, que EBIOS puede ser usada para estudiar tantos sistemas por diseñar, permitiendo determinar progresivamente las especificaciones de seguridad integrándose a la gestión de proyectos, como sistemas ya existentes considerando las medidas de seguridad existentes e integrando la seguridad a los sistemas en funcionamiento.

Contrariamente a los enfoques de análisis de riesgos por situaciones, el procedimiento estructurado del método EBIOS permite identificar los elementos constitutivos de los riesgos (entidades y vulnerabilidades, métodos de ataque y elementos peligrosos, elementos esenciales y necesidades de seguridad), garantizando la exhaustividad del análisis de riesgos (EBIOS Méthode de gestion des risqué, 2010, p. 14).

Por otro lado, EBIOS es compatible con las normas ISO/IEC 27001:2005, 15408, 17799, 13335 y 21827. Además, puede adaptarse al contexto de cada organización y ajustarse a sus herramientas y costumbres metodológicas, respetando la filosofía general del procedimiento; por lo que, puede realizar tanto un estudio global completo del sistema de información de una entidad como un estudio detallado de un sistema particular (sitio web, mensajería, etc.).

El método EBIOS se compone de cinco secciones adicionales o especies de libros; donde las secciones 3 y parte de la 4 comprende el análisis de riesgos y el resto es para la gestión del riesgo, que son:

1) **Sección 1 – Introducción:** En esta sección se presentan los enfoques de fondo, de interés y de posicionamiento. También contiene una bibliografía, un glosario y siglas.
2) **Sección 2 – Enfoque:** Esta sección describe la secuencia de actividades del método.

3) **Sección 3 – Técnica:** Esta sección sugiere formas de llevar a cabo las actividades del método. Será necesario adaptar estas técnicas a las necesidades y prácticas de la organización.
4) **Sección 4 - Herramientas para la evaluación de los riesgos SSI:** Esta sección es la primera parte de la base de conocimientos de EBIOS (tipos de entidades, los métodos de ataque, vulnerabilidades).
5) **Sección 5 - Medidas para el tratamiento del riesgo de SSI:** Esta sección es la segunda parte de la base de conocimientos EBIOS (objetivos de seguridad, requisitos de seguridad, tablas para la determinación de objetivos y requisitos funcionales de seguridad).

Cabe agregar que, el método EBIOS comprende cinco módulos para realizar su proceso de gestión de riesgos (ver figura 11) a saber:

Módulo 1: Contexto, el cual está diseñado para reunir todos los elementos necesarios para la gestión del riesgo, permite formalizar el marco de gestión de riesgo en el que se realizará el estudio, identificar, delimitar y describir el alcance del estudio y sus problemas, su contexto de uso y sus limitaciones especificas, en el cual se deben hacer preguntas como ¿Por qué y cómo vamos a manejar el riesgo?, ¿cuál es el objetivo del estudio?; además, este modulo involucra las siguientes actividades:

a) *Definir el marco de la gestión de riesgo:* aquí se identifica el área de estudio y se define el marco dentro del cual se realiza la gestión de riesgos. Donde, las acciones recomendadas son:
    i. Montar el estudio de riesgo.
    ii. Describir el contexto general.
    iii. Definir el alcance del estudio.
    iv. Identificar los parámetros a tener en cuenta.
    v. Identificar las fuentes de amenazas.

b) Preparar las métricas (indicadores): tiene como objetivo fijar el conjunto de los parámetros y de las escalas que servirán para administrar los riesgos; tiene como ventajas, garantizar la homogeneidad de las estimaciones y permite la repetitividad en el

tiempo de las actividades de gestión de los riesgos, cuyas acciones recomendadas son:

i. Definir los criterios de seguridad y elaborar las escalas de necesidades.
ii. Elaborar una escala de niveles de gravedad.
iii. Elaborar una escala de niveles de realidades.
iv. Definir los criterios de la gestión de los riesgos.

c) *Identificar los activos:* identificar los activos primordiales para la organización a través de las siguientes acciones:

i. Identificar los activos críticos, sus relaciones y sus propietarios.
ii. Identificar los activos soportes, sus relaciones y sus propietarios.
iii. Identificar las medidas de seguridad existentes.

Módulo 2: Reacciones adversas, Contribuye a la evaluación del riesgo, permite identificar y estimar las necesidades de seguridad de los activos (Disponibilidad, integridad, confidencialidad), y todos los impactos en caso de incumplirse estas necesidades. ¿Cuáles son las amenazas?, ¿cuáles son los problemas más graves?

Por otro lado, permite en primer lugar hacer emerger todos los incidentes de seguridad identificando y combinando cada uno de sus componentes: se estima así el valor de lo que se desea proteger (las necesidades de seguridad de los activos esenciales), se pone en evidencia las fuentes de amenazas con las cuales estamos confrontados y las consecuencias (impactos) de los siniestros. Involucra la siguiente actividad:

Módulo 3: Escenarios de amenazas, este módulo tiene como objetivo identificar de manera sistemática las amenazas. Permite en primer lugar hacer emerger todas las amenazas identificando y combinando cada uno de sus componentes: se pone en evidencia las diferentes amenazas, las fallas explotables para que se realicen (las vulnerabilidades de los activos secundarios), y las fuentes de amenazas.

También permite censar las medidas eventuales existentes de seguridad y estimar su efecto reestimando la verosimilitud de las amenazas, una vez las medidas aplicadas de seguridad. Al final de este módulo, las amenazas son identificadas, aclaradas y situadas unas con relación a otras en términos de verosimilitud.

Módulo 4: Riesgos, Consiste principalmente en cubrir las vulnerabilidades a las que está expuesta la entidad, es decir, disminuir los riesgos, resaltando y caracterizando los riesgos reales para el contexto establecido en el módulo 1.

Por otro lado, en este paso se realizan dos actividades importantes que son:

a) *Estimar los riesgos:* su propósito es poner en evidencia y caracterizar los riesgos reales; a través de las actividades: construir argumentos de manera simple y exhaustiva, justificar el uso de las medidas existentes de seguridad, evitar negociar argumentos que no constituyen riesgos y suministrar los datos necesarios para la evaluación de los riesgos.
b) *Identificar los objetivos de seguridad:* tiene como fin elegir cómo deben ser entendidos los riesgos en la evaluación y tiene como ventajas permitir elegir entre diferentes opciones que guían el tratamiento de los riesgos y establecer una especificación coherente con toda la información recogida durante todo el estudio. Además, se seleccionan las opciones que da el tratamiento de los riesgos y se analizan los riesgos residuales.

Módulo 5: Tratamiento del riesgo, este módulo tiene como objetivo identificar las formas de abordar los riesgos y controlar su aplicación, de acuerdo con el contexto del estudio, también se puede llegar a un consenso sobre las medidas de seguridad para hacer frente a los riesgos en función de los objetivos previamente identificados para demostrar la cobertura adecuada, y finalmente hacer la planificación, implementación y validación del tratamiento.

Al finalizar este módulo, se definen las medidas de seguridad y los puntos claves de manera formal. El módulo incluye las siguientes actividades: Formalizar las medidas de seguridad e implementarlas. De esta manera, el proceso de gestión de riesgos de la metodología EBIOS se muestra en la siguiente figura:

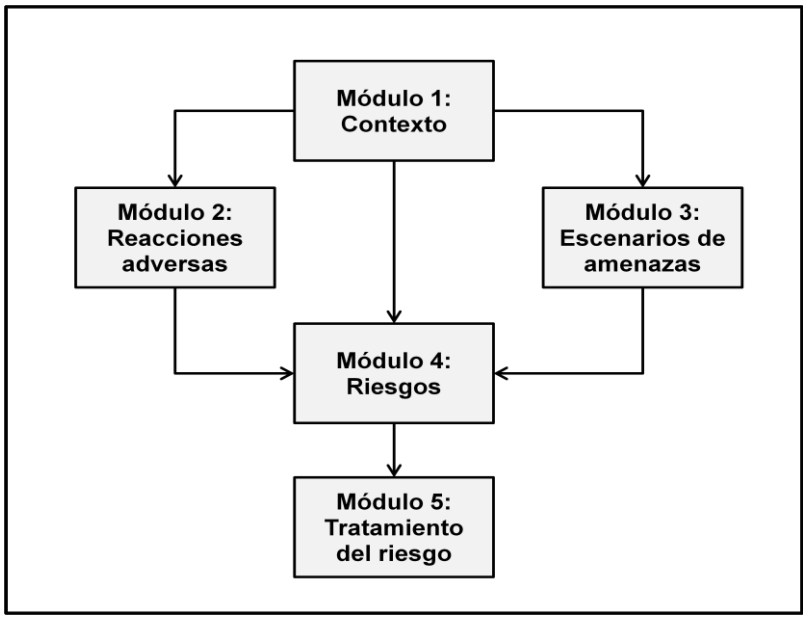


Figura 11: Proceso de gestión de riesgos de la metodología EBIOS
Fuente: EBIOS Méthode de gestion des risqué (2010)

Bases Legales

Los estándares internacionales y las leyes nacionales que tienen relación con esta investigación son los siguientes:

Estándares Internacionales

ISO/IEC 27001:2005 Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requerimientos.

ISO/IEC 27002:2005 Tecnología de la información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

ISO/IEC 27005:2008 Tecnología de la información – Técnicas de seguridad – Gestión de riesgos en la seguridad de la información.

Leyes nacionales

Ley especial contra delitos informáticos promulgada en Gaceta Oficial N° 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 el 12 de Junio del 2.000 y publicada en Gaceta Oficial N° 36.970, Caracas – Venezuela.

Sistema de variables

Stracuzzi y Pestana (2004) exponen que las variables "son elementos o factores que pueden ser clasificados en una o más categorías. Es posible medirlas o cuantificarlas, según sus propiedades o características" (p. 60); por lo que en una investigación las variables no son usadas como tal porque presentan un grado de abstracción, razón por la cual se deben operacionalizar, es decir, que deben ser manejadas, insertadas en cuadros y manipuladas en los instrumentos.

Se infiere entonces que, una variable puede verse como una cualidad susceptible a sufrir cambios, es decir, según lo expresan Hernández, Fernández y Baptista (2006), "es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse" (p. 123). Por lo tanto, las variables son los elementos que se van a medir, controlar y estudiar dentro del problema de investigación planteado.

Los autores explican que "sin definición de las variables no hay investigación… las variables deben ser definidas de forma conceptual y operacional…una definición conceptual trata a la variable con otros términos" (p. 145). Por otro lado, una definición operacional "especifica que actividades u operaciones deben realizarse para medir una variable" (p. 146).

Entonces, un sistema de variables está conformado por la definición conceptual y la definición operacional de cada una de las variables, es decir, las dimensiones y los indicadores de cada una de ellas. Es de hacer notar que la no presencia de hipótesis no implica la ausencia de variables en una investigación y además las variables deben ser medidas a través de los instrumentos de investigación (tests, pruebas, cuestionarios, entrevistas, entre otros).

Cuadro 1: Operacionalización de las variables

Variable	Dimensión	Indicadores	Instrumentos	Ítems	Fuente
Diseño de una Metodología para el Análisis de Riesgos en los Sistemas de Gestión de Seguridad de Información (SGSI) en las Universidades de Barquisimeto Estado Lara (MARISGSI)	1. **Seguridad de la Información:** definida por la norma ISO/IEC 27002:2005 como la protección de la información de un rango amplío de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.	• **Disponibilidad:** propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC 27001:2005)	a) Cuestionario b) Entrevista c) Observación directa	a1, a28, b14	a) Personal de los laboratorios de computación b) Administradores de red. c) Entorno
		• **Integridad:** Propiedad de salvaguardar la exactitud e integridad de los activos (ISO/IEC 27001:2005)		a25, a26, b28	
		• **Confidencialidad:** Propiedad que esa información este disponible y no sea divulgada a personas, entidades o procesos no-autorizados (ISO/IEC 27001:2005)		a2, a9, a24, a27, b26	
		• **No repudio:** servicio de seguridad que proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje u originado o haber sido el destinatario de una acción (Daltabuit Enrique, 2007).		a14, a35, b27	

Fuente: Autor (2010)

Sigue….

Continúa…

Variable	Dimensión	Indicadores	Instrumentos	Ítems	Fuente
Diseño de una Metodología para el Análisis de Riesgos en los Sistemas de Gestión de Seguridad de Información (SGSI) en las Universidades de Barquisimeto Estado Lara (MARISGSI)	**2. Sistema de Gestión de la Seguridad de Información (SGSI):** Consiste en la planificación, ejecución, verificación y mejora continua de un conjunto de controles y medidas, tanto técnicas como organizativas, que permitirán reducir el riesgo de sufrir incidentes de seguridad, dotando a la organización de un esquema de gestión sobre el cual desarrollar un plan director de seguridad de la información (López A., 2008)	• **ISO/IEC 27001:2005:** Estándar internacional que ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI (ISO/IEC 27001:2005) • **ISO/IEC 27002:2005:** Estándar internacional que proporciona las técnicas de seguridad, código para la práctica de la gestión de la seguridad de la información.	a) Cuestionario b) Entrevista c) Observación directa	a8, a10, a11, a31, b17 a3, a7, a23, a32, b24	a) Personal de los laboratorios de computación b) Administradores de red. c) Entorno

Fuente: Autor (2010)

Sigue…

Continua…

Variable	Dimensión	Indicadores	Instrumentos	Ítems	Fuente
Diseño de una Metodología para el Análisis de Riesgos en los Sistemas de Gestión de Seguridad de Información (SGSI) en las Universidades de Barquisimeto Estado Lara (MARISGSI)	**2. Sistema de Gestión de la Seguridad de Información (SGSI):** Consiste en la planificación, ejecución, verificación y mejora continua de un conjunto de controles y medidas, tanto técnicas como organizativas, que permitirán reducir el riesgo de sufrir incidentes de seguridad, dotando a la organización de un esquema de gestión sobre el cual desarrollar un plan director de seguridad de la información (López A., 2008)	• **Políticas de seguridad:** Dan cumplimiento a la misión de seguridad informática de una organización, ya que definen lo que está permitido y lo que está prohibido, los procedimientos y herramientas necesarias, expresan el consenso de los "dueños" y permiten adoptar una actitud de buen vecino en un entorno cada vez más globalizado (Daltabuit y Vázquez, 2007). • **ISO/IEC 27005:2008:** Proporciona directrices para la gestión de riesgos d seguridad de información. Es aplicable a todo tipo de organización. Está diseñada para ayudar a la aplicación satisfactoria de la seguridad de información basada en un enfoque de gestión de riesgos (ISO/IEC 27005:2008).	a) Cuestionario b) Entrevista c) Observación directa	a5, b4 a33, b19	a) Personal de los laboratorios de computación b) Administradores de red. c) Entorno

Fuente: Autor (2010)

Sigue…

Continua…

Variable	Dimensión	Indicadores	Instrumentos	Ítems	Fuente
Diseño de una Metodología para el Análisis de Riesgos en los Sistemas de Gestión de Seguridad de Información (SGSI) en las Universidades de Barquisimeto Estado Lara (MARISGSI)	3. **Análisis de Riesgos:** poderosa herramienta que permite establecer un marco sistemático que provee los indicadores adecuados para llevar acciones de control, mitigación o eliminación de peligros, riesgos e impactos adversos o no deseados en el transcurso de nuestras actividades, cualesquiera que éstas sean (Martínez 2002, p. 44)	• **Activos:** Cualquier cosa que tenga valor para la organización (ISO/IEC 27001:2005).	a) Cuestionario b) Entrevista c) Observación directa	a4, a13, a18, b1, b9, b25	a) Personal de los laboratorios de computación b) Administradores de red. c) Entorno
		• **Riesgos:** Combinación de la probabilidad de un evento y su ocurrencia (ISO/IEC 27002:2005).		a19, a38, b7, b13, b29	
		• **Vulnerabilidad:** La debilidad de un activo o grupo de activos que puede ser explotada por una o mas amenazas (ISO/IEC 27002:2005)		a15, a17, a36, b3, b5, b12, b15	
		• **Amenazas:** causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización (ISO/IEC 27002:2005).		a6, a20, a29, b2, b6, b20	
		• **Impacto:** Cambio adverso en el nivel de los objetivos de negocios llevada a cabo. (ISO/IEC 27005:2008).		a21, a22, a39, b10, b18	
		• **Salvaguardas:** O control, son los medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal (ISO/IEC 27002:2005).		a34, a37, b8, b30. b31	

Fuente: Autor (2010)

Sigue…

Continua…

Variable	Dimensión	Indicadores	Instrumentos	Ítems	Fuente
Diseño de una Metodología para el Análisis de Riesgos en los Sistemas de Gestión de Seguridad de Información (SGSI) en las Universidades de Barquisimeto Estado Lara (MARISGSI)	**4. Metodología para el Análisis de Riesgos:** conjunto de pasos que se usan para analizar los riesgos de un SGSI en una organización para dar cumplimiento a su misión, ejemplo de ellas son, CRAMM, MAGERIT, OCTAVE, etc. (Autor, 2011).	**Procedimientos:** acciones o tareas a realizar en relación a la ejecución de un proceso o actividad, debe ser claro, sencillo de interpretar y no ambiguo (Autor, 2012).	a) Cuestionario b) Entrevista c) Observación directa	a12, a16, a30, b11, b16, b21, b22, b23	a) Personal de los laboratorios de computación b) Administradores de red. c) Entorno

Fuente: Autor (2010)

CAPITULO III

MARCO METODOLOGICO

En este capítulo se define el conjunto de acciones destinadas a describir y analizar el problema de investigación planteado, a través de procedimientos específicos que incluyen las técnicas de observación y recolección de datos, para determinar el "cómo" se realizó la investigación para responder a los objetivos planteados; al respecto, Sabino (1992) comenta "en cuanto a los elementos que es necesario operacionalizar pueden dividirse en dos grandes campos que requieren un tratamiento diferenciado por su propia naturaleza: el universo y las variables" (p. 118).

En este sentido, la metodología aplicada para desarrollar el marco metodológico comprende la naturaleza de la investigación, el diseño de la investigación, población y muestra, técnicas e instrumentos de recolección de datos, validez y confiabilidad de los instrumentos y la técnica usada para el análisis de los datos.

Naturaleza de la investigación

De acuerdo al problema de investigación planteado y en función de sus objetivos, el estudio se emprendió siguiendo la modalidad de Proyecto Especial. Al respecto, el Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales, Normas UPEL (2006), expresa que este tipo de investigación permite la presentación de:

> Trabajos que lleven a creaciones tangibles, susceptibles de ser utilizadas como soluciones a problemas demostrados, o que respondan a necesidades e intereses de tipo cultural. Se incluye en esta categoría los trabajos de elaboración de libros de texto y de materiales de apoyo educativo, el desarrollo de software, prototipos y de productos tecnológicos en general… trabajos con objetivos y enfoques metodológicos no previstos en estas normas, que por su carácter innovador puedan producir un aporte significativo al acontecimiento sobre el tema seleccionado… (p. 22).

En el mismo orden de ideas, los proyectos especiales "están destinados a la creación de productos que puedan solucionar deficiencias evidenciadas, se caracterizan por su valor innovador y aporte significativo en cualquier área del conocimiento" (Stracuzzi y Pestana, 2004, p. 91).

Así, el proyecto especial se refiere al Diseño de una Metodología para el Análisis de Riesgos en los SGSI en las Universidades de Barquisimeto, Estado Lara; en función de los objetivos planteados, esta modalidad de investigación se apoyó en un diseño de investigación no experimental con un nivel descriptivo y una investigación de campo. Cabe citar a Sabino (1992), quien señala que una investigación de campo:

> Se basa en informaciones o datos primarios, obtenidos directamente de la realidad… para cerciorarse de las verdaderas condiciones en que se han conseguido sus datos, haciendo posible su revisión o modificación en el caso de que surjan dudas respecto a su calidad (p. 94).

Por otro lado, Stracuzzi y Pestana (2004) indican, que el diseño de investigación no experimental es aquel que:

> Se realiza sin manipular en forma deliberada ninguna variable…Se observan los hechos tal y como se presentan en su contexto real y en un tiempo determinado o no, para luego analizarlos. Por lo tanto, en este diseño no se construye una situación específica sino que se observan las que existen… (p. 81).

Arias (1997), plantea que el nivel de investigación se refiere "al grado de profundidad con que se aborda un objeto o fenómeno" (p. 47); por lo que, el nivel descriptivo consiste en la caracterización de un hecho o fenómeno con el fin de

establecer su estructura o comportamiento. Por otro lado, Stracuzzi y Pestana (2004), expresan que:

> Los estudios descriptivos pueden incluir hipótesis o no, según el objetivo que se persiga. El simple interés en conocer como marca una institución no amerita formulaciones hipotéticas; pero si lo que se pretende es demostrar algo, la formulación de hipótesis es pertinente y necesaria (p. 87).

Diseño de la investigación

En función del enfoque metodológico propuesto, el estudio abarcó las fases fundamentales en la formulación de un proyecto especial: Fase I Diagnóstico, Fase II Comparación y Fase III Diseño.

Fase I: Diagnóstico

En esta fase se revisó la bibliografía especializada en el tema de investigación, se diseño los instrumentos de recolección de datos para validarlos y luego aplicarlos al personal que labora en los laboratorios de computación y a los administradores de red de las instituciones UCLA, UNEXPO, UPEL, UNA, UFT, UNESR y UNY, para diagnosticar la necesidad de diseñar una metodología para el análisis de riesgos en los SGSI de las universidades de Barquisimeto Estado Lara. En este sentido, esta fase se estructura mediante el siguiente procedimiento:

1. Instrumentos de recolección de datos.
2. Validez y confiabilidad de los instrumentos.
3. Conclusiones del diagnóstico.
4. Recomendaciones del diagnóstico.

Población y muestra

Según Hernández, Fernández y Baptista (2006), la población es el conjunto de todos los casos que concuerdan con determinadas especificaciones y deben situarse claramente en torno a sus características de contenido, de lugar y en el tiempo. (p. 239). De la misma manera, Zapata (2006) expone, que población es el "conjunto de personas, sucesos o cosas con respecto a las cuales el investigador desea generalizar los resultados de su indagación" (p. 127). Se puede inferir que población es el conjunto total de elementos que poseen características comunes observables en un lugar y en un momento determinado.

Por otro lado, la muestra es definida por Hernández, Fernández y Baptista (2006) como el "subgrupo de la población del cual se recolectan los datos y debe ser representativo de dicha población" (p. 236).

De acuerdo a las definiciones anteriores, en esta investigación, la población para diseñar una metodología para el análisis de riesgos en los SGSI en las Universidades de Barquisimeto Estado Lara, estuvo constituida por 9 Administradores de Redes y 28 personas que laboran en los laboratorios de computación de las universidades en estudio, por consiguiente, por ser tan pequeña la población, se tomó como muestra la totalidad de la misma, así como lo muestra el cuadro 2.

En el transcurso de una investigación explica Moreno (2000) "es posible que ocurra una disminución de los números de sujetos; las razones de la disminución pueden ser diversas: enfermedad, desanimo, abandono voluntario, etc." (p. 88). Kerlinger y Lee (2002) lo describen como abandono o *mortandad experimental,* la cual se refiere al retiro de participantes por alguna causa y Fandos (2007) lo explica como "… la desaparición de integrantes de la muestra a lo largo de un tiempo por diversas causas" (p. 595).

Cuadro 2: Población y muestra

Sujetos participantes		Población Esperada (P)	Muestra Teórica (Mt)	% (Mt)	Muestra Aplicada (Ma)	% (Ma)	Tipo de selección	Instrumento/ Técnica
Administradores de red	**UNA**	1	1	1,00	1	1,00	Sin selección	Entrevista
	UNEXPO	2	2	1,00	2	1,00		
	UPEL	1	1	1,00	0	0		
	UCLA	1	1	1,00	1	1,00		
	UNY	1	1	1,00	0	0		
	UFT	1	1	1,00	1	1,00		
	UNESR	1	1	1,00	1	1,00		
Personal del laboratorio de computación	**UNA**	2	2	1,00	2	1,00	Sin selección	Cuestionario
	UNEXPO	4	4	1,00	4	1,00		
	UPEL	4	4	1,00	0	0		
	UCLA	10	10	1,00	5	0,50		
	UNY	3	3	1,00	2	0,66		
	UFT	4	4	1,00	2	0,25		
	UNESR	1	1	1,00	1	1,00		
		36 1,00	**36 1,00**		**22 0,611**			

Fuente: Oficina TIC Universidades (2012)

Instrumentos de recolección de datos

Hernández y otros (2006) explican que, "un instrumento de medición adecuado es aquel que registra datos observables que representan verdaderamente los conceptos o las variables que el investigador tiene en mente" (p. 276), además, los mismos autores opinan que, todo instrumento de recolección de datos debe reunir tres requisitos esenciales: *confiabilidad, validez y objetividad* (p. 277).

La *confiabilidad* es el grado en el que un instrumento produce resultados coherentes y consistentes (Hernández y otros, 2006, p. 277)

La *validez,* es el grado en el que un instrumento en verdad mide la variable que se busca medir (Hernández y otros, 2006, p. 278)

La *objetividad*, es el grado en que un instrumento es permeable a la influencia de los sesgos y tendencias de los investigadores que lo administran, califican e interpretan (Hernández y otros, 2006, p. 287).

Por consiguiente, se deduce que un instrumento es un mecanismo que usa el investigador para recabar y registrar la información pertinente al tema objeto de estudio. En función a los objetivos definidos en este estudio, así como la

operacionalización de las variables e indicadores, se elaboró un cuestionario (ANEXO B) que se aplicó al personal de los laboratorios de computación de las universidades en estudio, una entrevista (ANEXO C) a los administradores de red y la observación directa no participante y no estructurada en la realidad objeto de estudio.

Cuestionario

Stracuzzi y Pestana (2004) defininen el cuestionario como un instrumento que "tanto en su forma como en su contenido debe ser sencillo de contestar…las preguntas deben estar formuladas de manera clara y concisa; pueden ser cerradas o semiabiertas, procurando que la respuesta no sea ambigua" (p. 119).

Cabe considerar que, en este estudio el cuestionario se realizó usando la escala de Likert, método que fue desarrollado por Rensis Likert en 1932 y consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios, ante los cuales se pide la reacción de los participantes tal como lo indica Hernández y otros (2006). Ahora bien, la codificación de los datos en cada ítem y variable se estableció de la siguiente manera:

Cuadro 3: Codificación de los criterios del cuestionario

Categoría	Codificación (Valor asignado)
Definitivamente Sí	5
Probablemente Sí	4
Indeciso	3
Probablemente No	2
Definitivamente No	1

Es de hacer notar, que el instrumento estuvo constituido por 53 interrogantes inicialmente, quedando un total de ítems, luego de ser validado por los expertos, de 39 y se realizó usando 5 categorías de respuesta, de acuerdo a la codificación

previamente presentada. Por otro lado, con la finalidad de evitar que el orden en que se presentaron las alternativas llegara a afectar las respuestas de los sujetos, por ejemplo, tendencia a favorecer la primera o última respuesta, se convino en rotar el orden, realizando preguntas afirmativas y negativas, de manera de romper la continuidad de respuestas. Evidentemente, las ponderaciones se invirtieron para conservar la dirección de las afirmaciones, así como lo señala Hernández, Fernández y Baptista, 2006, "cuando las afirmaciones son negativas se califican al contrario de las positivas", en cuyos casos la escala para estos ítems fue de la forma siguiente:

Cuadro 4: Codificación inversa de los criterios del cuestionario

Categoría	Codificación (Valor asignado)
Definitivamente Sí	1
Probablemente Sí	2
Indeciso	3
Probablemente No	4
Definitivamente No	5

Entrevista

Sabino (1998) acota que, la entrevista "consiste en una interacción entre dos personas, una de las cuales (el investigador) formula determinadas preguntas relativas al tema de investigación, mientras que la otra (el investigado) proporciona verbalmente o por escrito la información que le es solicitada" (p. 146).

En este sentido, para esta investigación la entrevista estuvo constituida por 31 interrogantes abiertas, proporcionando una información más amplia sobre el problema de investigación, por lo cual profundizan una opinión o los motivos de un comportamiento (Hernández, Fernández y Baptista, 2008, p. 316).

Observación directa

Finalmente, la técnica de observación directa es conceptualizada cuando el investigador se pone en contacto personalmente con el hecho o fenómeno que trata de investigar (Stracuzzi y Pestana, 2004, p. 105), además, expresan que es no participante cuando se recoge la información desde afuera, sin intervenir en el grupo social, hecho o fenómeno investigado…y es no estructurada cuando se realiza con ayuda de elementos técnicos apropiados, tales como fichas, cuadros, tablas, entre otras (ob. cit., p. 106).

Validez y confiabilidad de los instrumentos

La validez es la cuestión más compleja que debe alcanzarse en todo instrumento de medición que se aplica, así lo expresa Hernández y otros (1997), y plantea la siguiente interrogante ¿Está usted midiendo lo que cree usted que está midiendo?; es decir, la validez es el grado en el que un instrumento en verdad mide la variable que se busca medir. Además, "la validez es un concepto del cual pueden tenerse diferentes tipos de evidencia: *evidencia relacionada con el contenido, con el criterio y con el constructo"* (Hernández y otros, 2006, p. 278).

En este orden de ideas se puede citar, a Hernández y otros (ob. cit.) que expresa "la validez de contenido se refiere al grado en que un instrumento refleja un dominio específico de contenido de lo que se mide" (p. 278). Es el grado en que la medición representa al concepto medido. Lo que quiere decir que, intenta evaluar la capacidad del instrumento para recoger el contenido y el alcance del constructo y de la dimensión.

De igual manera, Hernández y otros (ob. cit.) expresan que la "validez de criterio establece la validez de un instrumento de medición comparándola con algún criterio externo que pretende medir lo mismo" (p. 280). Es decir, que los resultados

obtenidos con el instrumento predicen o se relacionan con los resultados que se obtienen con otros instrumentos ya validados que miden un constructo similar.

Igualmente, los mismos autores establecen que la validez de constructo "se refiere a qué tan exitosamente un instrumento representa y mide un concepto teórico" (p. 282), además, se obtiene mediante el análisis de factores, porque nos indica cuántas dimensiones integran a una variable y que ítems conforman cada dimensión. En otras palabras, valida los fundamentos teóricos – conceptuales sobre los cuales se ha desarrollado el instrumento.

Sin embargo, Hernández y otros (ob. cit.) destacan otro tipo de validez que se llama "*validez de expertos* o *face validity*, la cual se refiere al grado en que aparentemente un instrumento de medición mide la variable en cuestión, de acuerdo con "voces calificadas"" (p. 284). Por lo que en este estudio el grupo de expertos estuvo conformado por la Msc. Luzneida Matute, docente de pregrado (Introducción a la computación), postgrado (administración de redes) y jefe del CTIC de la UCLA, Msc. Jesús Guedez, docente de pregrado (programación II) y postgrado (Arquitectura del computador) de la UCLA y Msc. Rosendo Mendoza, docente de pregrado (introducción a la computación) y jefe del departamento de sistemas de la UCLA.

En síntesis, la validez total de un instrumento se evalúa sobre la base de todos los tipos de evidencia. Cuanto mayor evidencia de validez de contenido, de criterio y de constructo tenga un instrumento de medición, éste se acercará más a representar las variables que pretende medir (Hernández y otros, 2006, p. 284).

Confiabilidad de los instrumentos de recolección de datos

Citando a Hernández, Fernández y Baptista (ob. cit.) "la confiabilidad de un instrumento de medición se refiere al grado en que su aplicación repetida al mismo sujeto u objeto produce resultados iguales" (p. 277). De esta manera, para evaluar la confiabilidad de un instrumento existen varias técnicas o métodos, entre las cuales la

más usada es la medida de coherencia interna usando el coeficiente alfa de Cronbach (α), que oscila entre 0 y 1, donde un coeficiente 0 significa nula confiabilidad y 1 representa un máximo de confiabilidad (confiabilidad total) (Hernández y otros, 2007, p. 439). También, expresan Hernández y otros (2007) que no hay regla que indique a partir de este valor no hay fiabilidad del instrumento. Más bien, el investigador calcula su valor, lo reporta y lo somete a escrutinio de otros investigadores. Pero se puede decir, de manera más o menos general, que si obtengo 0,25 de coeficiente, esto indica baja confiabilidad, si es 0,50 la fiabilidad es media, si supera el 0,75 es aceptable y si es mayor a 0,90 es elevada (p. 439).

En este sentido, para esta investigación se uso el programa computacional IBM SPSS Statistics 20 para calcular la confiabilidad del instrumento, el cual arrojó el siguiente resultado de coeficiente alfa de Cronbach:

$\alpha = 0{,}817$ lo que indica una confiabilidad aceptable.

Fase II: Comparación

De acuerdo con los objetivos planteados, en esta fase se procedió a comparar cinco metodologías para la gestión de riesgos existentes en el mercado internacional, como son MAGERIT, OCTAVE, EBIOS, MEHARI y CRAMM.

Cabe acotar, que la comparación se centro sólo en el proceso de *Análisis de riesgos*, el cual forma parte del proceso de **Gestión de riesgos.** En base a lo anterior, se tomó los indicadores que componen el proceso de *análisis de riesgos*, usando la definición de riesgo *basado en amenazas*/vulnerabilidades y que están fundamentados en la norma ISO/IEC 27005:2008, como son:

1) **Identificación del riesgo:**
    a. Identificación de activos.
    b. Identificación de amenazas.
    c. Identificación de controles existentes.

d. Identificación de vulnerabilidades.
e. Identificación de consecuencias.

2) Estimación del riesgo:

a. Metodologías de estimación de riesgos.
b. Valoración de consecuencias.
c. Valoración de la probabilidad del incidente
d. Estimación del nivel de riesgo.

Fase III: Diseño de la Metodología para el Análisis de Riesgos

Una vez completada la fase de comparación, se procedió a realizar el diseño de la Metodología para el Análisis de Riesgos en los SGSI en las Universidades de Barquisimeto Estado Lara, tomando como base el resultado de los criterios extraídos de las metodologías, los estándares y los hallazgos encontrados en el diagnóstico aplicado en la fase I.

CAPITULO IV

ANÁLISIS DE LOS DATOS

A continuación se presenta el análisis y la interpretación de los resultados obtenidos en la aplicación de los instrumentos empleados en esta investigación, cuyo propósito fue diseñar una metodología para el análisis de riesgos en los SGSI en las universidades de Barquisimeto Estado Lara.

En consecuencia, los datos obtenidos del instrumento cuestionario se ordenaron, procesaron, tabularon e interpretaron a través de las técnicas de porcentaje acumulado y la estadística descriptiva mediante la distribución de frecuencias, para relacionar las variables objeto de estudio. De esta manera, Hernández y otros (2007) expresan que una distribución de frecuencias "es un conjunto de puntuaciones ordenadas en sus respectivas categorías" (p. 419).

En este sentido, los datos referentes a la estadística descriptiva se plasmaron en una tabla de distribución de frecuencias y se obtuvo, a través del programa computacional IBM SPSS Statistics 20, los valores de *mínimo, máximo, media, moda, mediana, varianza, curtosis, rango* y los *percentiles 25, 50 y 75* con el propósito de explicar e interpretar su comportamiento expresando de manera clara y simple, usando la lógica inductiva y deductiva.

ANALISIS DE LOS DATOS RECABADOS EN EL CUESTIONARIO

DIMENSION/ INDICADOR	10	20	30	40	50	60	70	80	90	100
Seguridad de la información										
Disponibilidad										
1) ¿Cree que los servicios ofrecidos por los sistemas de información en la institución, están disponibles para sus usuarios cuando ellos así lo requieran?						o				
28) ¿La institución carece de políticas de seguridad que ofrezcan la disponibilidad de sus servicios de los SGSI?				o						
Integridad										
25) ¿Se han reportado casos donde la información contenida en los SGSI de la institución, ha sido robada o modificada sin autorización en los últimos 5 años?	o									
26) ¿Se han implementado técnicas de seguridad para garantizar la integridad de la información de los SGSI?					o					
Confidencialidad										
2) ¿En los últimos 5 años, la información disponible en los sistemas de información de la institución, ha sido divulgada, robada, mal utilizada o saboteada?		o								
9) ¿La información de los SGSI de la institución, es accedida por personas no autorizadas?						o				
24) ¿Conoce algún caso, en los últimos 5 años, donde la información que manejan los SGSI haya sido copiada por personas no autorizadas?	o									
27) ¿Se han implementado técnicas de seguridad para garantizar que la información de los SGSI solo pueda ser accedida por las partes autorizadas?							o			
No repudio										
14) ¿Cree Ud. Que el principio de No repudio de la información forma parte de la seguridad que maneja la institución en sus SGSI?			o							
35) ¿La institución toma en cuenta el principio de No repudio de la información como parte de la seguridad de los SGSI?		o								
MEDIA				o						

Gráfico 1: **Porcentaje acumulado,** Dimensión: **Seguridad de la información,** Indicadores: **Disponibilidad, Integridad, Confidencialidad y No repudio.**
Fuente: Autor (2012)

Análisis: En el gráfico que nos muestra el comportamiento de la dimensión seguridad de la información y sus indicadores: disponibilidad, integridad, confidencialidad y no repudio, se observa que los principios de integridad y no repudio son los que se encuentran más propensos a riesgos, mientras que la

confidencialidad y la disponibilidad manejan un nivel aceptable de seguridad. Según la información obtenida, se presentan muchos casos donde usuarios no autorizados acceden, hurtan, modifican la información de los sistemas. En líneas generales las instituciones deben implementar políticas de seguridad que permitan asegurar los activos principales, como la información (correos electrónicos, páginas web, documentos, bases de datos, faxes, presentaciones, etc.); teniendo presente que existe una gran diferencia entre seguridad informática y seguridad de la información, ya que según la muestra, toman medidas en relación a la seguridad de la infraestructura de las tecnologías de la información más que de la seguridad de los activos.

DIMENSION/ INDICADOR	10	20	30	40	50	60	70	80	90	100
SGSI										
ISO/IEC 27001:2005										
8) ¿Conoce el estándar ISO/IEC 27001:2005, que proporciona los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI?										
10) ¿Se aplican los requerimientos especificados en el estándar 27001:2005 en los SGSI de la institución?										
11) ¿Dentro de la documentación importante que maneja la institución existe el documento de la norma ISO/IEC 27001:2005?										
31) ¿Se desconoce la norma ISO/IEC 27001:2005 para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI?										
ISO/IEC 27002:2005										
3) ¿Considera que la institución implementa estrategias de seguridad que cubran los procesos donde la información es el activo principal?										
7) ¿Tiene conocimiento de la existencia del código de buenas prácticas para la gestión de la seguridad de la información (Estándar ISO/IEC 27002:2005)?										
23) ¿Tiene conocimiento sobre cuáles son los objetivos de control especificados en el estándar ISO/IEC 27002:2005, que usa la institución para la seguridad de la información?										
32) ¿Existe una supervisión en el uso de la norma ISO/IEC 27002:2005, que permita el incremento de la calidad operativa de la institución?										
Políticas de seguridad										
5) ¿El personal de la institución conoce las políticas de seguridad manejada para sus SGSI?										
ISO/IEC 27005:2008										
33) ¿La institución prevé los riesgos reales de los SGSI permitiendo la aplicación de la norma ISO/IEC 27005:2008?										
MEDIA										

Gráfico 2: **porcentaje acumulado,** Dimensión: **Sistemas de Gestión de la Seguridad de Información (SGSI),** Indicadores: **ISO/IEC 27001:2005, ISO/IEC 27002:2005, Políticas de seguridad, ISO/IEC 27005:2008**
Fuente: Autor (2012)

Análisis: Se observa en el gráfico que en las instituciones no conocen, ni implementan la norma ISO/IEC 27001:2005 que especifica los requerimientos para

establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI; es decir, los SGSI de las entidades no se fundamentan en esta norma. Por otro lado, existe una discrepancia con el indicador ISO/IEC 27002:2005, porque los sujetos indican que no tienen conocimiento de la existencia de sus controles para la gestión de la seguridad de la información, pero afirman que existe una supervisión en el uso del estándar que permite el incremento de la calidad operativa de las instituciones.

Así mismo, los sujetos afirman que se aplica la norma ISO/IEC 27005:2008, que es una guía para la gestión de los riesgos de seguridad de la información de acuerdo con los principios definidos en las normas ISO/IEC 27001:2005 e ISO/IEC 27002:2005, para prever riesgos tanto externos como internos a las instituciones en sus sistemas de información. Es de hacer notar, que para un mejor entendimiento de este estándar se deben conocer las normas ISO/IEC 27001:2005 e ISO/IEC 27002:2005.

Además, se observa que el personal de las instituciones no tiene conocimiento de la existencia de las políticas de seguridad que se implementan para mantener seguros los activos. Por lo que, es recomendable que todo el personal de las instituciones sepan de la existencia y contenido del manual de políticas de seguridad de la información, porque proporciona una guía clara de la dirección para la seguridad de la información en relación a los objetivos y requisitos de las entidades, leyes y regulaciones relevantes y pertinentes.

Por último, se puede inferir según la data recopilada, que las instituciones en estudio no cuentan con Sistemas de Gestión de Seguridad de la Información (SGSI) para garantizar la seguridad de la información. Por lo tanto, es recomendable implementar SGSI porque permite, en primer lugar, analizar y ordenar la estructura de las instituciones; en segundo lugar, facilitará la definición de procedimientos de trabajo para mantener su seguridad; y por último, ofrece la posibilidad de disponer de controles que permitan medir la eficacia de las medidas tomadas, lo que permite proteger a las entidades frente a amenazas y riesgos que puedan poner en peligro los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de las mismas.

DIMENSION/ INDICADOR	10	20	30	40	50	60	70	80	90	100
ANALISIS DE RIESGOS										
ACTIVOS										
4) ¿Considera que la institución tiene codificados los activos principales de sus sistemas de sus Sistemas de Gestión de Seguridad de la Información (SGSI)?										
13) ¿Considera que los activos principales de los SGSI se encuentran protegidos contra posibles amenazas?										
18) ¿La institución tiene identificados y registrados los activos principales de los SGSI?										
RIESGOS										
19) ¿Se tienen claramente identificados los riesgos a los que están expuestos los activos de los SGSI?										
38) ¿La carencia de principios de seguridad de la información permite identificar los riesgos presentes en los SGSI?										
VULNERABILIDAD										
15)¿En los últimos 5 años, algún activo de los SGSI ha sido vulnerado?										
17) ¿La institución lleva un registro de las vulnerabilidades que se han presentado en los SGSI en los últimos 5 años?										
36) ¿El histórico de los casos relacionados con vulnerabilidades de los SGSI de la institución en los últimos 5 años, se encuentra debidamente archivado?										
AMENAZAS										
6) ¿La institución ha resuelto satisfactoriamente las amenazas presentadas en los últimos 5 años, en sus SGSI?										
20) ¿Se lleva un registro de las amenazas que se han detectado en los últimos 5 años en los activos de los SGSI?										
29) ¿La institución evalúa el grado en que pueden ser afectados sus activos por las amenazas identificadas?										
IMPACTO										
21) ¿Se ha estimado el impacto que tendría en la institución, la falta de existencia de un proceso de análisis de riesgos a los SGSI?										
22) ¿Se usa algún método definido para determinar el impacto que causa una amenaza en los activos de los SGSI de la institución?										
39) ¿La aplicación de los procedimientos de seguridad prevén el impacto de posibles riesgos en los SGSI?										
SALVAGUARDAS (CONTROLES)										
34) ¿La institución toma medidas de protección (salvaguardas) sobre sus activos?										
37) ¿La institución carece de mecanismos o salvaguardas para la protección de sus activos?										
MEDIA										

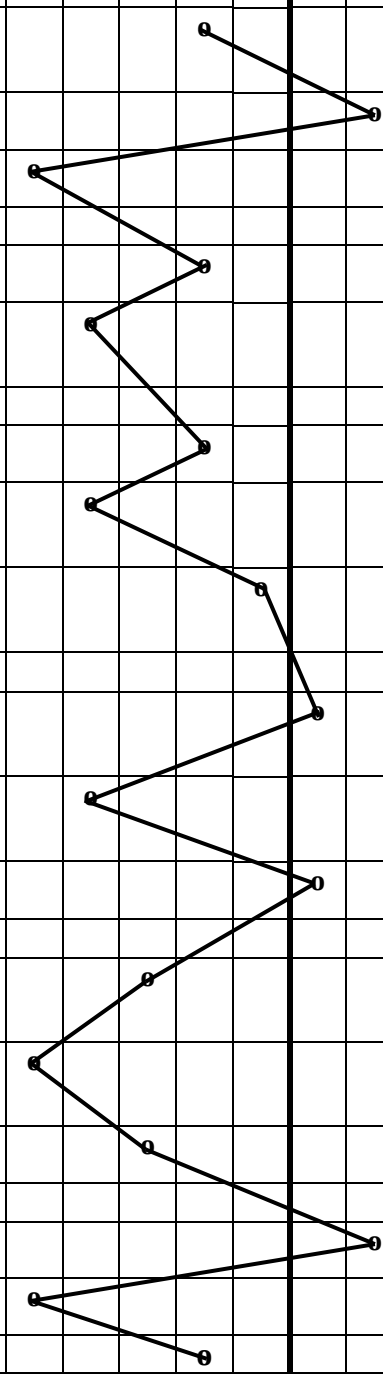


Gráfico 3: **Porcentaje acumulado,** Dimensión: **Análisis de riesgo,** Indicador: **Activos, riesgos, vulnerabilidad, amenazas, impacto, salvaguardas.**
Fuente: Autor (2012)

Análisis: Se observa que, los activos no se encuentran debidamente identificados, codificados y registrados. Se debe tener claro, que los activos es todo aquello que es importante, primordial y fundamental para el cumplimiento de los objetivos de las organizaciones; siendo la información el activo principal a proteger. Por lo tanto, las instituciones deben elaborar y mantener un inventario de los activos de información donde se muestre el propietario (directivo o gestores responsables de protegerlos) y los detalles relevantes (ubicación, nº serie, nº de versión, etc.).

Por otro lado, no se llevan registros de las vulnerabilidades que han presentado los activos de información y de las amenazas detectadas en los mismos; pero se nota que los incidentes con amenazas los han resuelto de alguna manera.

Por lo tanto, las instituciones en relación al análisis de riesgos se encuentran en un nivel bajo, porque no tienen identificados los riesgos de seguridad, no determinan su magnitud para implantar los controles necesarios para minimizarlos. Es decir, no realizan el proceso de análisis de riesgos, lo que es curioso y cabe preguntarse cómo determinan los riesgos a los que están sometidos sus activos de información.

DIMENSION/ INDICADOR	10	20	30	40	50	60	70	80	90	100
METODOLOGIA PARA EL ANALISIS DE RIESGOS										
PROCEDIMIENTOS										
12) ¿En los últimos 5 años la institución ha manejado algún procedimiento para analizar los riesgos presentados en sus SGSI?										
16) ¿Considera importante que la institución cuente con un procedimiento para realizar el análisis de riesgos a los SGSI?										
30) ¿La institución ha usado procedimientos, normas, estándares, para resolver satisfactoriamente los peligros que acechan a los SGSI?										
MEDIA										

Gráfico 4: **Porcentaje acumulado,** Dimensión: **Metodología para el análisis de riesgos**
Indicadores: Procedimientos
Fuente: Autor (2012)

Análisis: Se observa en el gráfico, que las instituciones en estudio no implementan ni cuentan con procedimientos para realizar el proceso de análisis de riesgos.

También, se percibe un completo interés en poseer procedimientos o métodos que les permitan asegurar lo más posible los activos fundamentales para la operatividad de las instituciones.

MEDIA / DIMENSION	10	20	30	40	50	60	70	80	90	100
Seguridad de la información										
SGSI										
Análisis de riesgos										
Metodología para análisis de riesgos										

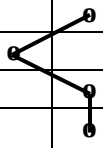


Gráfico 5: **Porcentaje acumulado,** Variable: **Diseño de una metodología para el análisis de riesgos en los sistemas de gestión de seguridad de la información (SGSI) en las universidades de Barquisimeto Estado Lara.**
Fuente: Autor (2012)

Análisis: De este gráfico general, se puede decir que las instituciones se encuentran por debajo de la media en referencia al tema de seguridad. Por lo cual, la fase de análisis de riesgos, que es una parte de la seguridad de la información en general, es importante porque permite identificar todos los activos importantes para la seguridad de los sistemas de gestión de seguridad de la información (SGSI), para identificar las amenazas que puedan afectarles, para identificar la vulnerabilidad de cada uno de ellos frente a estas amenazas y para calcular el riesgo existente de un posible impacto sobre el activo. Así, los responsables de la seguridad de la información pueden tomar las decisiones pertinentes para implantar medidas de seguridad optimizando el factor riesgo-inversión.

Por lo tanto, es importante y necesario que las instituciones cuenten con una metodología que les permita mantener seguros los activos principales de sus sistemas de gestión de seguridad de la información (SGSI).

Análisis estadístico descriptivo

A continuación se presenta el análisis estadístico descriptivo del instrumento cuestionario, el cual se realizó usando el programa computacional IBM SPSS Statistics 2.0 para obtener los siguientes datos:

Cuadro 5: Estadístico descriptivo del cuestionario

	N	x	Mo	Md	s^2	Min	Máx	Rango	Curtosis	A_s	P_{25}	P_{50}	P_{75}
Personal laboratorios computación	16	112,8	107	109	136,8	97	138	41	-,201	,625	104,7	109	122,5

Cuadro 6: Tabla de distribución de frecuencias

INTERVALOS	X_i	f_i	F_i	f_r	F_{ra}
39 - 71	55	0	0	0	0
72 - 104	88	4	4	0,25	0,25
105 - 137	121	11	15	0,688	0,938
138 - 170	154	1	16	0,063	1
171 - 203	187	0	16	0	1

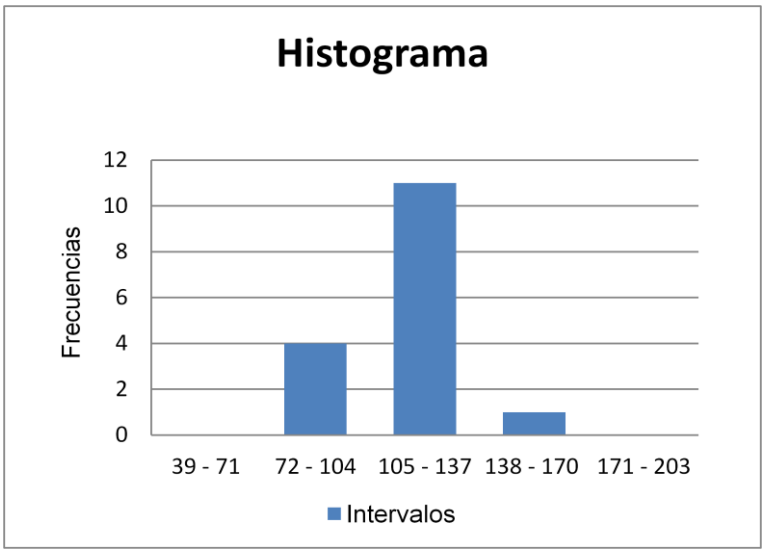
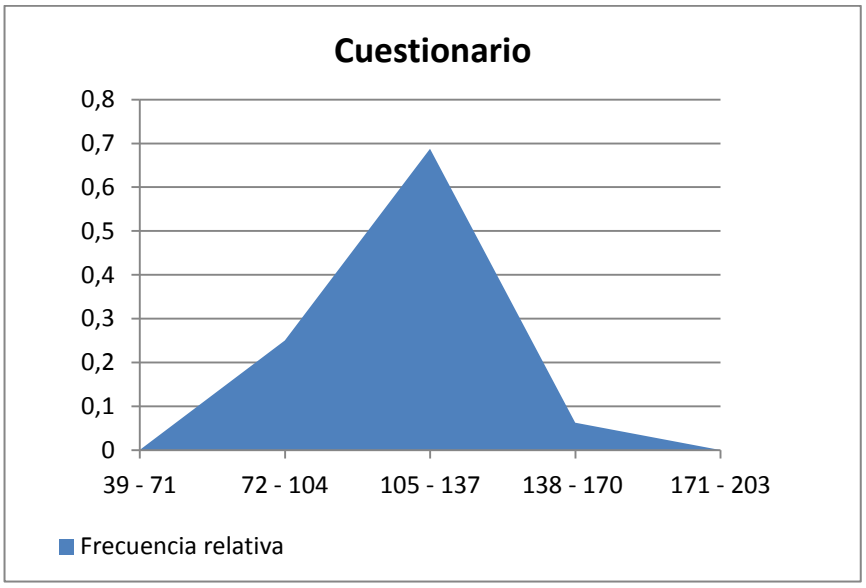


Gráfico 6: **Histograma de la tabla de distribución de frecuencias**



Conclusiones del diagnóstico

En líneas generales, se puede concluir que:

1) Las universidades en estudio no cuentan con un manual de políticas de seguridad, por lo que, las medidas de seguridad que manejan son temporales, es decir, cuando ocurre el incidente buscan la solución correctiva basándose en experiencias pasadas.
2) El personal directivo y gerencial no participan activamente en las decisiones que se toman referentes a los riesgos que corren los sistemas de información de sus instituciones.
3) No se informa al personal de la institución sobre las medidas de seguridad que se toman cuando ocurren fallas de seguridad.
4) No se capacita a los usuarios para el buen manejo de los servicios que ofrecen las instituciones a su comunidad estudiantil.
5) No se capacita al personal para el buen manejo de la información de sus sistemas.
6) Falta de personal capacitado para controlar y hacer seguimiento a los SGSI.
7) Algunas instituciones tienen claro el nivel de riesgos que presentan sus sistemas, pero por la falta de presupuesto y coordinación gerencial, no se han implementado políticas de seguridad.
8) No existe bitácoras de amenazas y por consiguiente tampoco de las soluciones.
9) No existe bitácoras de las vulnerabilidades que han encontrado en sus sistemas.
10) No existe, dentro de la documentación importante para mantener seguros los activos principales de la institución, los estándares ISO/IEC 27001:2005, ISO/IEC 27002:2005 e ISO/IEC 27005:2008 que ofrecen lineamientos de seguridad a las organizaciones de cualquier tipo, tamaño y actividad económica.
11) No se aplican las normas para la gestión de la seguridad de la información ISO/IEC 27001:2005, ISO/IEC 27002:2005 e ISO/IEC 27005:2008.

12) No han realizado una evaluación del impacto que supondría la materialización de una amenaza en los activos más importantes.
13) Al no tener políticas de seguridad, no manejan controles o salvaguardas para tratar los riesgos que se presentan en los sistemas.
14) No realizan procedimientos de análisis de riesgos en sus sistemas, ni aplican metodologías comerciales para ello.
15) Las instituciones en estudio mostraron gran interés en contar con una metodología para el análisis de riesgos en los SGSI y el poder aplicarla.

En este sentido, las conclusiones son coherentes con los datos recopilados en los instrumentos aplicados a las instituciones objeto de estudio, concluyendo que, el diseño de la metodología para el análisis de riesgos de los SGSI es necesario para mantener una buena gestión en la seguridad de la información.

ANÁLISIS DE LOS DATOS RECABADOS EN LA ENTREVISTA

Cuadro 7: Dimensión: **Seguridad de la información;** Indicadores: **Disponibilidad, integridad, confidencialidad y no repudio**

ÍTEM	RESPUESTA	ANALISIS
14) ¿Cree que los servicios ofrecidos por los sistemas de información en la institución, están disponibles para sus usuarios cuando ellos así lo requieran, explique?	**Sujeto 1:** si lo están, siempre se cuenta con disponibilidad de conexión, mientras no se presenten amenazas. **Sujeto 2:** si están disponibles mientras no existan fallas eléctricas. **Sujeto 3:** casi siempre. Cuando no están disponibles es por problemas con el proveedor. **Sujeto 4:** si, con mucha frecuencia, nunca es el 100%. **Sujeto 5:** En este núcleo, la mayoría de las veces solo el de internet. Todo lo demás es manejado por Caracas. **Sujeto 6:** Sí. La mayoría está a la disposición, sólo falta adiestramiento a los usuarios.	Las respuestas indican que las instituciones no le han dado la importancia que la seguridad de la información tiene como una función empresarial más dentro de la entidad, tomando en cuenta que la disponibilidad, integridad, confidencialidad y no repudio de la información deben garantizarse; así como también el cumplimiento con las normativas legales vigentes. En cuanto a la propiedad de disponibilidad, los usuarios indican que el servicio de internet generalmente está disponible a sus usuarios siempre y cuando no se presenten fallas o amenazas. No indicaron disponibilidad en otros servicios. También, se observa que la propiedad de integridad y confidencialidad han sido alteradas con frecuencia por personas no autorizadas; es decir, la información disponible en algunos sistemas ha sido divulgada, modificada, hurtada, etc. En este sentido, se puede concluir que la información que manejan los sistemas de las instituciones en estudio carece de medidas de seguridad efectivas. Con referencia a lo anterior, la norma ISO/IEC 27001:2005 define seguridad de información como "preservación de la confidencialidad, integridad y disponibilidad de la información, además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad" (p. 10). Por lo tanto, es recomendable redefinir las medidas de seguridad que se tienen para minimizar los riesgos a los que está expuesta tal información, y para darle cumplimiento a ese propósito se sugiere el uso de la norma ISO/IEC 27001:2005 para garantizar su funcionamiento de manera efectiva.
28) ¿Se han reportado casos donde la información contenida en los SGSI de la institución, ha sido borrada o modificada sin autorización en los últimos 5 años, explique?	**Sujeto 1:** No **Sujeto 2:** Si. No explico los casos. **Sujeto 3:** Si, en el sistema de estudios a distancia porque la página web fue modificada por un usuario no autorizado externo. **Sujeto 4:** a nivel de usuario por desconocimiento. **Sujeto 5:** no respondió. **Sujeto 6:** Desconozco.	
26) ¿En los últimos 5 años, la información disponible en los sistemas de información de la institución, ha sido divulgada, robada, mal utilizada o saboteada?	**Sujeto 1:** No. **Sujeto 2:** Si. **Sujeto 3:** No. **Sujeto 4:** A nivel de usuario se filtra información, por desconocimiento de políticas de seguridad por parte del usuario. **Sujeto 539:** No respondió. **Sujeto 6:** Probablemente sí.	
27) ¿Considera que el principio de No repudio de la información forma parte de la seguridad que maneja la institución en sus SGSI, explique?	**Sujeto 1:** No, en ningún caso hay manera de detectar interrupción en la comunicación por alguna de las partes. **Sujeto 2:** En algunos servicios, tales como el correo electrónico. **Sujeto 3:** No. **Sujeto 4:** No. **Sujeto 5:** no respondió. **Sujeto 6:** Definitivamente, puesto que el no repudio es prueba de la integridad y del origen de los datos, ambos en una relación infalsificable que pueden ser verificados por un tercero en cualquier momento.	

Fuente: Autor (2012)

Dimensión: Sistemas de Gestión de la Seguridad de la Información (SGSI)
Indicadores: ISO/IEC 27001:2005, ISO/IEC 27002:2005, Políticas de seguridad e ISO/IEC 27005:2008

ÍTEM	RESPUESTA	ANALISIS
17) ¿Aplica la institución la norma ISO/IEC 27001:2005 para mantener seguros sus SGSI, explique?	**Sujeto 1:** No. **Sujeto 2:** No. **Sujeto 3:** No. **Sujeto 4:** No. **Sujeto 5:** no respondió. **Sujeto 6:** Probablemente no.	En cuanto a la dimensión Sistemas de Gestión de Seguridad de la Información (SGSI), se observa según las respuestas de los entrevistados que las instituciones no usan ni aplican las normas ISO/IEC 27001:2005, ISO/IEC 27002:2005 e ISO/IEC 27005:2008 para asegurar la información y los sistemas que la procesan. En este sentido, las instituciones deben fundamentarse en los estándares de seguridad para mantener en un nivel confiable la información que se maneja en sus sistemas. Es así, que la norma ISO/IEC 27001:2005 especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI; permitiendo a la organización priorizar y seleccionar los controles en base a sus posibilidades y necesidades. Por lo tanto, se recomienda implementar la norma ISO/IEC 27001:2005 ya que está diseñada para asegurar la selección adecuada y proporcionar los controles de seguridad que protejan los activos de los SGSI. Por otro lado, la norma ISO/IEC 27002:2005 indica que "la seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio y minimizar el riesgo comercial" (p. 8). Por lo tanto, se debe tomar en cuenta este estándar como guía para conocer qué se puede hacer para mejorar la seguridad de la información. También, se observa que las instituciones educativas en estudio carecen de un manual de políticas de seguridad evidenciando la inexistencia de controles que permitan garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de las entidades; por lo que no se cumple con lo expresado en la norma ISO/IEC 27002:2005, "es esencial que una organización identifique sus requerimientos de seguridad" (p. 9), así como "el documento de la política de seguridad de la información debiera ser aprobado por la gerencia, publicado y comunicado a todos los empleados y las partes externas relevantes" (p. 20); por lo que se recomienda tomar como base fundamental para crear el manual de políticas de seguridad la norma ISO/IEC 27002:2005 en su apartado 5.
24) ¿La institución aplica la norma ISO/IEC 27002:2005 como guía para la gestión de la seguridad de la información. Explique?	**Sujeto 1:** No. **Sujeto 2:** No. **Sujeto 3:** No. Desconozco el estándar. **Sujeto 4:** No **Sujeto 5:** No respondió. **Sujeto 6:** Probablemente no.	
15) ¿Cuenta la institución con un manual de políticas de seguridad vigentes para mantener seguros sus SGSI, con qué frecuencia lo aplica?	**Sujeto 1:** No tenemos **Sujeto 2:** Si existe, pero está incompleto y no se aplica. **Sujeto 3:** No tenemos **Sujeto 4:** no tenemos **Sujeto 5:** no tenemos. **Sujeto 6:** desconozco si existe un manual de seguridad vigente.	
1) ¿Se aplica el estándar ISO/IEC 27005:2008 para el análisis de riesgos en los SGSI, explique cómo?	**Sujeto 1:** No. **Sujeto 2:** No. **Sujeto 3:** No. Desconozco el estándar. **Sujeto 4:** No **Sujeto 5:** No respondió. **Sujeto 6:** Probablemente no.	

Fuente: Autor (2012)

Dimensión: Análisis de riesgos
Indicador: Activos

ÍTEM	RESPUESTA	ANALISIS
28) Describa cuáles son los activos principales que posee la institución. ¿Están protegidos?	**Sujeto 1:** switch, router, servidores, modem, Access point. Algunos están protegidos. **Sujeto 2:** servidores, router, switch administrables. Algunos están protegidos. **Sujeto 3:** switch, router, servidores, modem. Comenta que existe un nivel muy bajo de protección. **Sujeto 4:** Información en general, si está protegida y está clasificada por nivel de seguridad, tienen un directorio activo (grupos y dominios) para el control de acceso, esto es que cada usuario tiene un login y una contraseña y además manejan los permisos para los usuarios. Indica que a nivel físico los equipos están protegidos. Manejan respaldos. **Sujeto 5:** sistemas de información SIACE, la información del sistema INVISION POWER BOARD. La información se encuentra protegida a nivel medio. **Sujeto 6:** Normativa, leyes, actas de consejo, comunicaciones internas, información del personal docente, administrativo, obrero y estudiantil. Libros, tesis, investigaciones, trabajos de ascenso, infraestructura, equipos de computación, mobiliario, material de oficina. Están parcialmente protegidos.	Con respecto a los activos hay diversidad de opiniones entre los entrevistados, para unos los activos sólo son los equipos que procesan la información (switch, router, modem, servidores, etc.); mientras que para otros, los activos es la información sin importar como se encuentra disponible (papel, digital, etc.). En este sentido, la norma ISO/IEC 27002:2005 aclara que activo es "cualquier cosa que tenga valor para la organización" (p. 13), y agregando lo expresado por Daltabuit y otros (2007) "… entre otras cosas se debe considerar: hardware, software, datos, documentación, servicios u operación" (p. 248). Por otro lado, se observa que los activos físicos son los que se encuentran identificados, inventariados y codificados en la mayoría de las instituciones; y lo hacen de forma manual en una hoja de cálculo en Excel, almacenando el número del activo, nombre, procedencia, ubicación, etc. Pero, los activos de información no lo están, lo cual hace difícil establecer un nivel de seguridad y tratamiento de la información adecuados. De lo anterior, se deduce que las instituciones en estudio dan más importancia a los activos físicos (de hardware) que a la información; por lo que se recomienda hacer una descripción completa y detallada de los activos y además tratarlos conforme a su nivel de criticidad para la consecución de los objetivos de negocio, tomando en cuenta que los activos con mayor valor contable no son necesariamente los más críticos, para efectos de un análisis de riesgos se deben valorar no sólo teniendo en cuenta su valor de adquisición o reposición, sino también el costo inducido por la materialización de una amenaza, así como se menciona en la metodología MAGERIT.
9) ¿Están todos los activos principales claramente inventariados, de qué manera?	**Sujeto 1:** si lo están, se tienen en un archivo en Excel. **Sujeto 2:** si lo están, se tienen listados con un código en un archivo en Excel. **Sujeto 3:** los activos de software no se tienen inventariados, mientras que los físicos si lo están, se llevan en un formato en Excel y actualmente se hace un sistema para ello. **Sujeto 4:** físicamente si lo están, codificados con Nº, nombre activo, indica de donde proviene, indica donde se encuentra actualmente. Los activos de información no lo están de manera escrita, pero conocemos cuales son los sistemas más críticos y que se deben resguardar más. **Sujeto 5:** no lo están. Todo está centralizado en Caracas. **Sujeto 6:** Si. Están identificados y codificados.	
29) ¿La institución tiene identificados y registrados los activos principales de los SGSI. Cómo?	**Sujeto 1:** no. **Sujeto 2:** Si.. no dio explicación de cómo. **Sujeto 3:** A nivel físico sí, pero no de manera escrita y formal; y a nivel de sistemas no. **Sujeto 4:** Físicamente si, y se lleva en una hoja de Excel. **Sujeto 5:** No respondió. **Sujeto 6:** Probablemente sí.	

Fuente: Autor (2012)

Dimensión: Análisis de riesgos
Indicador: Riesgos

ÍTEM	RESPUESTA	ANALISIS
7) ¿Realiza la institución un análisis de riesgos a sus SGSI? Explique cómo lo hace.	**Sujeto 1:** no se hace. **Sujeto 2:** No se realiza **Sujeto 3:** formalmente no. **Sujeto 4:** no se hace. **Sujeto 5:** no se hace **Sujeto 6:** Desconozco el procedimiento	Los sujetos entrevistados dejaron claro que en las instituciones no se realiza análisis de riesgos, aunque si conocen el nivel de riesgos que tienen los activos de los sistemas. Estos indican que por falta de presupuesto y coordinación gerencial no se implementan medidas de seguridad para contrarrestar los riesgos que se presentan. Cabe destacar, que los riesgos ordenan los incidentes según su probabilidad de que ocurran y estas estimaciones pueden priorizar los riesgos y concentrarse en aquellas cosas más probables y/o que traigan las peores consecuencias. En algunas ocasiones, el riesgo es un indicador del estado de seguridad de los activos y sirve para tomar decisiones; en fin, el riesgo mide lo que puede pasar. En teoría, riesgo es definido por la norma ISO/IEC 27005:2008 como "el potencial de que una amenaza determinada aproveche las vulnerabilidades de un activo o grupo de activos y con ello cause daño a la organización" (p. 1). En este sentido, un análisis de riesgos esta antecedido por el inventario de los activos y de las amenazas, luego se debe calificar cada escenario posible para conocer su impacto y su riesgo; por lo que, es lógico que las instituciones no realicen este proceso cuando no se ha hecho el inventario de los activos y amenazas correspondientes. Por lo tanto, se recomienda que para realizar un correcto proceso de análisis de riesgos, las entidades deben hacer lo siguiente: a) Identificar, inventariar y codificar los activos más importantes. b) Identificar las amenazas a las que se exponen los activos c) Identificar las vulnerabilidades que explotan las amenazas d) Estimar el impacto causado por la materialización de las amenazas e) Establecer e implementar los controles necesarios para mitigar los riesgos. Cabe agregar, que es importante que la dirección de las instituciones debe implicarse a la hora de realizar un proceso de análisis de riesgos, ya que, las decisiones sobre lo que se debe hacer con los riesgos las debe tomar el equipo directivo y gerencial. Además, todo el personal debe tener conocimiento de dicho proceso para saber cómo tratar los activos de los que son propietarios.
13) ¿En los últimos 5 años se ha realizado algún proceso para calcular la magnitud de los riesgos, explique?	**Sujeto 1:** no **Sujeto 2:** no **Sujeto 3:** no **Sujeto 4:** no **Sujeto 5:** no respondió. **Sujeto 6:** Probablemente sí. Desconozco el proceso.	
29) ¿Se tiene claro el nivel de riesgo que tienen los activos de los SGSI de la institución, explique?	**Sujeto 1:** Si se tiene claro pero falta presupuesto, coordinación, entre otras, no se han implementado políticas de seguridad. **Sujeto 2:** Si. **Sujeto 3:** No. **Sujeto 4:** No. Porque la parte directiva no está al tanto de los activos y la seguridad. **Sujeto 5:** No respondió. **Sujeto 6:** Probablemente sí, puesto que se implementan algunos controles.	

Fuente: Autor (2012)

Dimensión: Análisis de riesgos
Indicador: Amenazas

ÍTEM	RESPUESTA	ANALISIS
2) Indique la frecuencia con que se presentan las amenazas en los activos de los Sistemas de Gestión de Seguridad de la Información (SGSI). Describa esas amenazas.	**Sujeto 1:** La frecuencia es media, las amenazas que se han presentado son virus, problemas eléctricos por falta de aterramiento, inundaciones. **Sujeto 2:** La frecuencia es media, tomando en cuenta que los equipos no se encuentran bien protegidos. Los problemas que hemos tenido con los equipos son por la electricidad (tableros principales). **Sujeto 3:** La frecuencia es media, los problemas más fuertes que hemos presentado son hackeos a los servidores web y a los servidores de correo. **Sujeto 4:** la frecuencia es intermedia tanto en equipos como en la información manejada. Hemos presentado problemas de phising y denegación de servicio. A veces los usuarios borran archivos. **Sujeto 5:** Esporádica, mayormente cuando hay cambio de personal, los problemas presentados son información perdida o eliminada, saboteos en los sistemas. **Sujeto 6:** Con relativa frecuencia.	La información recopilada indica que la frecuencia con que se presentan las amenazas en los activos de los SGSI es intermedia y generalmente son fallas en la electricidad, virus, hackeos a servicios públicos, denegación de servicio y mal manejo de la información por parte del usuario. En este sentido, amenaza es definida como una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización (ISO/IEC 27002:2005, p. 15), cabe agregar que las amenazas existen porque los activos son vulnerables a diversos incidentes que surgen a través de fallas de seguridad; consecuencia de no implementar procedimientos de análisis de riesgos, ya que éste aporta objetividad a los criterios en los que se apoya la seguridad y se centra en proteger los activos más críticos y permite a las entidades gestionar los riesgos por sí mismas, apoyando la toma de decisiones basándose en los riesgos propios. Por otro lado, se evidencia que al no presentar políticas de seguridad, tampoco exista un manual de procedimientos que se pueda aplicar cuando ocurra un incidente amenazante ante los activos de los SGSI; por lo que, las respuestas de los entrevistados indican que los incidentes se resuelven en el momento en que ocurren y por experiencias pasadas; es decir, la solución generalmente es correctiva más que preventiva. En efecto, este indicador muestra una que existe la necesidad de crear una metodología para el análisis de riesgo que se aplique en un período de tiempo para revisar como se encuentra la seguridad de los SGSI atendiendo a la identificación de amenazas y vulnerabilidades en los activos principales de la institución. En fin, se recomienda que las instituciones universitarias fundamenten estos procesos de análisis de riesgos en la norma ISO/IEC 27005:2008 para tomar los requerimientos referentes a la gestión del riesgo; tendiendo claro que no sirve de metodología para realizar el proceso.
16) Explique, ¿cuál es el procedimiento que realizan cuando un SGSI es afectado por alguna amenaza?	**Sujeto 1:** no se aplica ninguno. **Sujeto 2:** No hay procedimiento alguno. Solo resuelven en el momento por descarte. **Sujeto 3:** No tenemos procedimiento escrito como tal, se procede a revisar el historial de los servidores, cambiar claves de usuarios, revisar los firewall de cada PC y modificar políticas de firewall. **Sujeto 4:** No tenemos manual, todo es empírico, por experiencias. Se procede a buscar el origen del problema por descarte. **Sujeto 5:** no tenemos. **Sujeto 6:** Mayor control en los accesos a usuarios	
2) ¿Considera que los activos principales de los SGSI se encuentran protegidos contra posibles amenazas, explique cómo?	**Sujeto 1:** no. **Sujeto 2:** No. **Sujeto 3:** Si, la parte física están bien resguardados la mayoría de los equipos. A nivel de sistemas constan de niveles de acceso, respaldos, autenticación por contraseña. **Sujeto 4:** Físicamente si, y a nivel de sistemas también, porque son protegidos por niveles de acceso, autenticación, permisos y respaldos. **Sujeto 5:** lo desconoce, porque todo lo maneja Caracas. **Sujeto 6:** Probablemente no.	

Fuente: Autor (2012)

Dimensión: Análisis de riesgos
Indicador: Vulnerabilidad

ÍTEM	RESPUESTA	ANALISIS
3) Describa las vulnerabilidades que han presentado los SGSI en la institución en los últimos 5 años. ¿Con qué frecuencia se presentan?	**Sujeto 1:** No se cuenta con políticas de administración de la información. La frecuencia es intermedia. **Sujeto 2:** Virus con una frecuencia intermedia. **Sujeto 3:** fraude en el sistema de pagos, borrado de información, virus. El fraude paso una vez, los demás problemas suceden de vez en cuando. **Sujeto 4:** Principalmente física: electricidad, también han presentado phising en los servidores. **Sujeto 5:** falta de personal responsable que lleve el control de los SGSI. **Sujeto 6:** personas que se hacen pasar por otras en registro académico, estudiantes que quieren acceder al servidor principal para aumentar su cuota de impresión, hurto.	Se observa que la frecuencia con la que se presentan las vulnerabilidades en los activos es intermedia, al igual que las amenazas. También, es notorio que las entidades no llevan un registro de las vulnerabilidades encontradas y tampoco una bitácora con las recomendaciones, porque no realizan análisis de vulnerabilidades por no poseer procedimientos para ejecutar el proceso de análisis de riesgos. Cabe destacar que los sistemas que son más vulnerables son los servidores de correo electrónico y web por ser servicios públicos; así como también el sistema de control de estudios. Esto indica que se tiene conocimiento de cuáles son los sistemas más vulnerables, pero por carecer de un método para realizar el proceso de análisis de riesgos que permita conocer claramente cuáles son esas vulnerabilidades que pueden ser explotadas por amenazas, no se establecen ni implementan los controles adecuados para mitigar los riesgos que éstas puedan causar a los activos, sino que se actúa en el momento del incidente. En este sentido, vulnerabilidad es definida por la norma ISO/IEC 27002:2005 como la "debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas" (p. 15). Con referencia a lo anterior, es recomendable que las instituciones opten por crear sus manuales de políticas de seguridad y aplicar métodos para análisis de riesgos tomando como bases las normas ISO/IEC 27002:2005 e ISO/IEC 27005:2008, las cuales sirven de guía para establecer un procedimiento de análisis de riesgos más no es en sí misma una metodología.
17) Describa cuáles de los SGSI que maneja la institución son más vulnerables y ¿por qué?	**Sujeto 1:** ninguno **Sujeto 2:** lo desconoce **Sujeto 3:** el servidor de correo y el servidor web, porque son servicios públicos y son fácilmente modificables por un tercero. **Sujeto 4:** Los sistemas públicos como los servicios web y los de correo electrónico. Porque tienen acceso a ellos personas no autorizadas. **Sujeto 5:** El sistema de control de estudios **Sujeto 6:** Desconozco los SGSI que maneja la institución.	
12) ¿Existe una bitácora de recomendaciones sobre los análisis de vulnerabilidades realizados en la institución en los últimos 5 años?	**Sujeto 1:** No. **Sujeto 2:** No. **Sujeto 3:** No. Sólo se hace un informe trimestral de lo sucedido en ese tiempo. **Sujeto 4:** No. **Sujeto 5:** no respondió. **Sujeto 6:** Probablemente sí. Desconozco el resultado	
18) ¿En los últimos 5 años, se ha realizado un análisis de vulnerabilidades de sus SGSI. Cuál fue el resultado?	**Sujeto 1:** no. **Sujeto 2:** No. **Sujeto 3:** No. **Sujeto 4:** No. **Sujeto 5:** lo desconoce, porque todo lo maneja Caracas. **Sujeto 6:** Probablemente sí. Desconozco el proceso.	

Fuente: Autor (2012)

Dimensión: Análisis de riesgos
Indicador: Impacto

ÍTEM	RESPUESTA	ANALISIS
10) ¿En los últimos 5 años, se han identificado los impactos que han tenido las pérdidas de confidencialidad, integridad, disponibilidad y no repudio sobre los activos de la institución?	**Sujeto 1:** no. **Sujeto 2:** No. **Sujeto 3:** No. **Sujeto 4:** No. **Sujeto 5:** lo desconoce, porque todo lo maneja Caracas. **Sujeto 6:** Probablemente sí.	Con referencia a todo lo anterior, y a las respuestas obtenidas por los entrevistados en este indicador, se concluye que al no existir un método para hacer análisis de riesgo en los SGSI, pues se hace difícil hacer una estimación de los impactos. Resulta oportuno, expresar que a pesar de que han sufrido riesgos importantes los SGSI de las instituciones, y se han resuelto por experiencias pasadas y por análisis empíricos, no se tiene registro alguno de ellos y por lo tanto no se ha estimado el impacto que han tenido esas amenazas sobre los activos. Por otro lado, los entrevistados indican que existen activos físicos que se han eliminado o cambiado, no por el alto impacto que han tenido, sino por obsoletos; en igual forma, se han eliminado servidores de correo electrónico porque el ancho de banda colapso, lo cual generaba un impacto en el servicio. En este orden de ideas, la forma más sencilla de hacer un análisis de impacto es imaginarse las consecuencias de que haya un incidente, sea accidental o deliberado; es decir, responderse preguntas como: ¿Qué pasaría si se revela un dato confidencial?, ¿Qué pasaría si manipulan la información de nuestros sistemas?, ¿Qué pasaría si la institución se queda sin servicio durante horas?, etc. Esto dará una idea del daño que pueda derivarse de una falla de seguridad, es decir, el impacto mide lo que puede pasar. Teóricamente, el impacto es la consecuencia de la materialización de una amenaza en un activo, o como lo define la norma ISO/IEC 27005:2008 "un cambio adverso en los objetivos de la organización" (p. 1). Por lo tanto, se recomienda llevar un registro de los incidentes y la estimación del impacto para que al momento de realizar un análisis de riesgos se incluyan para posteriores análisis y de esta manera ir comparando el nivel de riesgo en la organización a medida que se va mejorando el SGSI; todo esto con la ayuda de la metodología para análisis de riesgos.
18) ¿Se han presentado situaciones en los últimos 5 años, donde se han eliminado activos debido al alto impacto que éstos provocan sobre la misión de la institución?	**Sujeto 1:** no **Sujeto 2:** no **Sujeto 3:** no. La parte física se cambia ya porque los equipos están viejos, obsoletos. **Sujeto 4:** no. Ahora lo que sí ha sucedido es que se eliminó el servidor de correo porque el ancho de banda colapsaba y la capacidad. **Sujeto 5:** no respondió. **Sujeto 6:** Probablemente no.	

Fuente: Autor (2012)

Dimensión: Análisis de riesgos
Indicador: Salvaguardas (controles)

ÍTEM	RESPUESTA	ANALISIS
8) ¿Cuándo se han presentado los riesgos en los SGSI, se ha determinado que salvaguardas (controles) hay dispuestos y cuan eficaces son frente a esos riesgos? Explique.	**Sujeto 1:** no aplica. **Sujeto 2:** no aplica. **Sujeto 3:** solo se mantienen respaldos y los controles son mínimos. **Sujeto 4:** como no tenemos políticas, no tenemos controles específicos sino que, en caso de problemas, pues buscamos el origen del problema y lo resolvemos con lo aprendido en experiencias pasadas. **Sujeto 5:** no respondió. **Sujeto 6:** no respondió.	Los sujetos entrevistados indican que en líneas generales, los controles que se toman en cuenta para mitigar los riesgos presentados en sus SGSI son en su mayoría correctivos, consecuencia de carecer de políticas de seguridad y de métodos o procedimientos estandarizados,; es decir, correctivos porque cuando aparece el riesgo se ataca buscando su origen y se procede a resolverlo usando experiencias similares; sin embargo, existen otros pocos que usan los controles preventivos como codificaciones, distribución, resguardo en discos externos, uso de servidores en la nube, etc. En este orden de ideas, y para clarificar se indica la definición teórica de salvaguarda según Daltabuit y otros (2007) que expresan que "es una medida de protección (técnica o normativa) de los activos informáticos" (p. 248); es decir, son las prácticas, procedimientos o mecanismos que reducen el riesgo y éstas pueden actuar disminuyendo el impacto o la probabilidad. Por lo tanto, se recomienda aplicar los controles preventivos para minimizar los riesgos en los sistemas, para ello pueden fundamentarse en los estándares ISO/IEC 27005:2008 y 27002:2005 en sus apartados de gestión de riesgos, adaptándolos a las necesidades de las instituciones.
30) ¿Describa los controles aplicados a los SGSI para reducir la exposición al riesgo protegiendo los activos principales de la institución?	**Sujeto 1:** Ninguno. **Sujeto 2:** No se aplica. **Sujeto 3:** No tienen. **Sujeto 4:** Ninguno de estándar, empíricamente y experiencia. **Sujeto 5:** No respondió. **Sujeto 6:** Codificaciones, distribución, resguardo en discos externos, uso de servidores en la nube.	
31) ¿En los últimos 5 años, los controles usados para reducir los riesgos en los SGSI han sido correctivos o preventivos, explique?	**Sujeto 1:** Ninguno. **Sujeto 2:** Correctivos sin planificación y sobre la marcha **Sujeto 3:** Preventivos y correctivos. **Sujeto 4:** Ambos, pero se usan más los correctivos. **Sujeto 5:** No respondió. **Sujeto 6:** correctivos. Cuando aparece un riesgo se ataca. Poco se previene.	

Fuente: Autor (2012)

Dimensión: Metodología para el análisis de riesgos
Indicador: Procedimientos

ÍTEM	RESPUESTA	ANALISIS
11) ¿La institución usa algún procedimiento para realizar análisis de riesgos a los SGSI, cuál?	**Sujeto 1:** no. **Sujeto 2:** No. **Sujeto 3:** No. **Sujeto 4:** No. **Sujeto 5:** lo desconoce, porque todo lo maneja Caracas. **Sujeto 6:** Probablemente sí. Desconozco el procedimiento.	Según los entrevistados, ninguna de las instituciones en estudio cuenta con alguna metodología para realizar el proceso de análisis de riesgos, por lo que se puede inferir entonces que estas entidades no han realizado tal proceso por lo menos de manera formal y estricta porque no existe un registro como tal. Cuando se les preguntó si conocían algunas metodologías comerciales para el análisis de riesgos, la mayoría respondió que no tenían conocimiento, otros indicaron que si conocían algunas pero no lo suficientemente como para aplicarlas; entre las más nombradas están OCTAVE y MAGERIT, dos de las metodologías que se están comparando en esta investigación. Por otro lado, los sujetos mostraron gran interés en el diseño de una metodología para análisis de riesgos en los SGSI, porque sus respuestas fueron: si, porque: a) Ayuda a proteger los recursos que no deben ser afectados. b) Es indispensable por la alta cantidad de procesos que maneja la institución c) Hay un análisis formal de los riesgos y se puede ver y saber que políticas y controles usar para mitigarlos d) No tienen una y les daría más organización y eficiencia. e) Además hay que difundirla a la comunidad universitaria. Por lo antes expuesto, se recomienda contar y aplicar con la metodología para el análisis de riesgos en los SGSI producto de esta investigación; ya que se adapta a las necesidades de las instituciones universitarias públicas y privadas; además de ser una solución a los problemas de riesgos que en ellas se presentan a diario.
19) ¿La mayoría de las amenazas presentadas en los SGSI de la institución han sido solucionadas a través de algún procedimiento de análisis de riesgos. Explique el procedimiento aplicado?	**Sujeto 1:** no. **Sujeto 2:** No. **Sujeto 3:** No. Ningún procedimiento en específico, sino todo por intuición y experiencia. Mucho ensayo y error. **Sujeto 4:** No. **Sujeto 5:** lo desconoce, porque todo lo maneja Caracas. **Sujeto 6:** Probablemente sí. Desconozco el procedimiento.	
3) ¿Conoce cuáles son las metodologías existentes en el mercado para realizar el análisis de riesgos a los SGSI. Explique?	**Sujeto 1:** Las específicas en la norma ISO 27002, y algunas herramientas del mercado como MAGERIT y OCTAVE. **Sujeto 2:** OCTAVE, METRICA3, COBRA. **Sujeto 3:** No. **Sujeto 4:** No tengo idea. **Sujeto 5:** No. **Sujeto 6:** No. Conozco algunas pero no lo suficiente como para aplicarlas.	
4) ¿Implementan alguna de las metodologías existentes en el mercado para el análisis de riesgos en la institución. Indique cuál?	**Sujeto 1:** No, ninguna. **Sujeto 2:** No. **Sujeto 3:** No. **Sujeto 4:** No. **Sujeto 5:** no respondió. **Sujeto 6:** Probablemente sí. Desconozco cuál.	
5) ¿Considera necesario diseñar una metodología para el análisis de riesgos en los SGSI de la institución para mitigar o corregir los riesgos en los SGSI. Explique por qué?	**Sujeto 1:** Si, porque nos ayuda a proteger los recursos que no deben ser afectados. **Sujeto 2:** Si, porque para una institución como ésta, con una alta cantidad de procesos en producción es indispensable. **Sujeto 3:** Si, es bueno y recomendable porque así hay un análisis formal de los riesgos y se puede ver y saber que políticas y controles usar para mitigarlos. **Sujeto 4:** Si, porque no tenemos una. También porque nos da más organización y más eficiencia. **Sujeto 5:** no respondió. **Sujeto 6:** Por supuesto, sobre todo difundirla a la comunidad universitaria.	

Fuente: Autor (2012)

FASE II: COMPARACION DE LAS METODOLOGIAS MAGERIT, CRAMM, EBIOS, MEHARI Y OCTAVE

En esta fase se procedió a comparar cinco metodologías internacionales y comerciales a saber: MAGERIT, CRAMM, OCTAVE, MEHARI y EBIOS, para lo cual se tomó en consideración sólo el procedimiento para realizar el proceso de *análisis de riesgos*, el cual forma parte de la *gestión de riesgos*.

En este sentido, la comparación se centró en cómo las metodologías mencionadas ejecutan cada paso que se sigue para cumplir con un análisis de riesgos; por lo cual, los criterios tomados teniendo como referencia la norma ISO/IEC 27005, son los que se siguen en el enfoque de riesgo basado en amenazas/vulnerabilidades, que se mencionan a continuación:

Análisis de riesgos: Los dos pasos más importantes son:

1) **Identificación del riesgo,** dentro del cual se encuentran:
    a. Identificación de activos.
    b. Identificación de amenazas.
    c. Identificación de controles existentes.
    d. Identificación de vulnerabilidades.
2) **Estimación del riesgo,** se tienen:
    a. Metodologías de estimación de riesgo.
    b. Valoración de consecuencias.
    c. Valoración de la probabilidad del incidente.
    d. Estimación del nivel de riesgo.

Cuadro 8: **Comparación de las metodologías MAGERIT, MEHARI, OCTAVE, CRAMM Y EBIOS**

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
INFORMACIÓN 3GENERAL	**Nombre:** C.C.T.A Risk Analisys and Management Method (Metodología de gestión y análisis de riesgos.	**Nombre:** MEthod for Hamornized Analisys of Risk.	**Nombre:** Expression des Besoins et Identification des Objectifs de Sécurité (Expresión de necesidades e identificación de objetivos de seguridad)	**Nombre:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.	**Nombre:** Operationally Critical Threat, Asset, and Vulnerability Evaluation.
	País de origen: United Kingdom	**País de origen:** Francia	**País de origen:** Francia	**País de origen:** España	**País de origen:** USA
	Desarrollada por: Organización gubernamental / públicas British CCTA (Central Communication and Telecommunication Agency)	**Desarrollada por:** Organización sector privado / asociación (CLUSIF: Club for the Security of Information in France)	**Desarrollada por:** Organización sector privado, asociaciones, públicas y organizaciones gubernamentales (Club EBIOS, más de 60 empresas, ministerios franceses y expertos independientes.	**Desarrollada por:** Organización gubernamental (Ministerio de Administraciones Públicas).	**Desarrollada por:** Organización pública / gubernamental. (Carnegie Mellon University (USA), CERT (Computer Emergency Response Team))
	Fecha 1º versión: 1985 **Fecha última versión:** 2003 (V5)	**Fecha 1º versión:** 1998 **Fecha última versión:** 2010, MEHARI 2010	**Fecha 1º versión:** 1995 **Fecha última versión:** 2004 (V2)	**Fecha 1º versión:** 1997 (V1) **Fecha última versión:** 2005 (V2)	**Fecha 1º versión:** 1999 (V0.9) **Fecha última versión:** 2005 (V2.0)

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
INFORMACIÓN GENERAL	**Sitio web oficial:** www.cramm.com **Lenguajes disponibles:** Inglés, Holandés, Checo. **Modalidad:** Desconocida **Ámbito de aplicación:** Gobierno, Organismos, compañías grandes. **Uso:** Administración, operacional y técnico.	**Sitio web oficial:** www.clusif.asso.fr **Lenguajes disponibles:** Inglés, Francés. **Modalidad:** Libre (La solución está desarrollada en código abierto, libre de cargo). **Ámbito de aplicación:** Gobierno, Organismos, empresas medianas y grandes, compañías comerciales, sin fines de lucro (educación, salud, servicios públicos, Organizaciones no gubernamentales). **Uso:** Administración (Administrador principal, gerentes).	**Sitio web oficial:** www.ssi.gouv.fr **Lenguajes disponibles:** Inglés, Francés, Alemán, Español. **Modalidad:** libre **Ámbito de aplicación:** Gobierno, Organismos, Compañías grandes, PYME, Compañías comerciales y no comerciales. **Uso:** Administración, operacional.	**Sitio web oficial:** www.csi.map.es **Lenguajes disponibles:** Español, Inglés, Italiano. **Modalidad:** Libre **Ámbito de aplicación:** Gobierno, Organismos, compañías grandes, PYME, compañías comerciales y no comerciales. **Uso:** Administración, operacional y técnico.	**Sitio web oficial:** www.cert.org/octave **Lenguajes disponibles:** Inglés. **Modalidad:** Libre **Ámbito de aplicación:** PYME **Uso:** Administración, operacional.

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
DESCRIPCIÓN GENERAL	Es una metodología de análisis de riesgos que se debe usar obligatoriamente con la herramienta del mismo nombre CRAMM. Las primeras versiones tanto de la metodología como de la herramienta, se basaron en las mejores prácticas de las organizaciones gubernamentales británicas. En la actualidad, CRAMM es el método de análisis de riesgos preferido del gobierno de UK. Es apropiada para organizaciones grandes, gubernamentales e industriales.	Es un método de Análisis y Gestión del Riesgo que incluye en las bases de conocimiento las fórmulas para la evaluación directa de los riesgos y la selección de las formas para reducirlos. Las bases de conocimiento están disponibles como un libro (Excel y Open Office) capaz de llevar a cabo la cualificación y cuantificación de todos los elementos de riesgos. Proporciona un modelo de gestión de riesgos compatible con los requerimientos de la ISO/IEC 27005:2008. Incluye la clasificación de los activos, la probabilidad de las amenazas, medidas de vulnerabilidades a través de la auditoria. Basa su análisis en parámetros y fórmulas.	Es un conjunto completo de guías (más una herramienta de software libre) dedicada a la gestión de riesgos en los sistemas de información. Es usada en el sector público y privado de Francia y el extranjero. Es compatible con los principales estándares de seguridad de TI. Es una herramienta flexible que produce una amplia gama de productos (objetivos de seguridad, perfiles de protección, planes de acción, etc.). Consiste en un ciclo de 5 fases, donde las 3 primeras son de análisis del riesgo y las 2 últimas son de gestión del riesgo.	Metodología abierta para el Análisis y Gestión del riesgo que pretende alcanzar los siguientes objetivos: Que los responsables de los sistemas de información sean conscientes de la existencia de riesgos y de la necesidad de tratarlos a tiempo; ofrecer un método sistemático para tratar los riesgos; ayudar a describir y planificar las medidas apropiadas para mantener los riesgos bajo control; preparar a la organización para la evaluación, auditorias, procesos de certificación o acreditación, según sea el caso. Está estructurada en 3 libros: Metodología, catálogo de elementos y técnicas prácticas.	Metodología de Análisis y Gestión del riesgo, que define una evaluación estratégica basada en riesgos y la planificación técnica de la seguridad; es auto dirigida, es decir, que las personas de una organización asuman la responsabilidad de establecer la estrategia de seguridad de la entidad. OCTAVE-S es dirigida por un pequeño e interdisciplinario equipo (3 a 5 personas) del personal de la entidad para recopilar y analizar la información, produciendo planes de estrategias para mitigar los riesgos. Es una metodología para empresas pequeñas (< 100 empleados.)

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
HERRAMIENTAS Y COMPATIBILIDAD CON LOS ESTÁNDARES ISO/IEC	Soporta herramientas **Comerciales:** ❖ CRAMM Expert ❖ CRAMM Express Es compatible con el estándar: ISO/IEC 17799, actualmente ISO/IEC 27002:2005	Soporta herramientas: **No comerciales:** Un primer nivel de la herramienta está incluida en la base de conocimientos del método, usando formulas de Excel y open office. Un manual de referencia explica el uso, el cual es libre. **Comerciales:** RISICARE de BUC SA. Es compatible: ❖ Originalmente con el estándar ISO/IEC IS 13335-1. ❖ Luego evolucionó a MEHARI 2010 y cumple con los requisitos de la ISO/IEC 27005:2008. ❖ ISO/IEC 27001:2005	Soporta herramientas: **No comerciales:** libres (Open Source). Es compatible con las normas: ISO/IEC 27001:2005 ISO/IEC 15408 ISO/IEC 17799 ISO/IEC 13335 ISO/IEC 21827	Soporta las herramientas: **No comerciales:** PILAR **Comerciales:** EAR Es compatible con: ISO/IEC 27001:2005 ISO/IEC 15408:2005 ISO/IEC 17799:2005 ISO/IEC 13335:2004	Soporta herramientas: **Comerciales:** ❖ Material licenciado. ❖ Entrenamientos (sectores con disponibilidad: apoyo educativo, talleres de sensibilización). No tiene compatibilidad con estándares.

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
FASES DEL METODO: ANÁLISIS DE RIESGOS	Definición de riesgo basado en *activo/amenazas* o *amenazas/ vulnerabilidad* **a) Identificación de riesgos:** identificación y valoración de activos, identificación de amenazas, controles existentes, vulnerabilidades. b) **Estimación del riesgo:** Selección y recomendación de medidas de prevención.	Definición de riesgo basado en *escenarios* El proceso de identificación de riesgos se logra en gran parte a través de la base de conocimientos. a) **Establecimiento del contexto** (escenario) **b) Tipología y lista de activos principales.** c) **Análisis de activos:** activos de respaldo y vulnerabilidades intrínsecas. d) **Daños potenciales:** lista de posibles escenarios de riesgos. e) **Análisis de amenazas:** eventos de iniciación, actores, condiciones específicas. f) **Elementos de reducción de riesgos:** servicios de seguridad relevantes, beneficios de los servicios de seguridad.	Definición de riesgo basado en *escenarios* **a) Identificación del riesgo:** estudio de fuentes de amenazas, de vulnerabilidades, formalización de amenazas y justificación para descartarlas, oportunidad de riesgo y consecuencias de este. **b) Estimación del riesgo:**	Definición de riesgo basado en *activo/amenazas* o *amenazas/ vulnerabilidad* a) **Identificar activos:** activos relevantes, su interrelación y valoración. **b) Identificar amenazas** c) **Determinar las salvaguardas** que hay dispuestas y cuan eficaces son frente al riesgo. d) **Estimar el impacto:** daño sobre el activo derivado de la materialización de la amenaza. e) **Estimar el riesgo:** impacto ponderado con la tasa de ocurrencia de la amenaza.	Definición de riesgo basado en *activo/amenazas* o *amenazas/ vulnerabilidad* a) **Identificación del riesgo:** solo criterios. b) **Análisis de riesgos:** solo criterios c) **Evaluación del riesgo:** solo criterios

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
ACTIVOS	**Identificación de activos:** • Físicos • Software (Aplicaciones) • Datos (Información contenida en los sistemas de información). **Valorar los activos:** Los físicos se valoran en términos de costo de reemplazo. El software y los datos se valoran en términos del impacto que se produciría si la información fuera a estar no disponible, destruida, divulgada o modificada.	**Identificación del escenario (situación) de riesgo:** Existen 2 formas principales de identificar los riesgos: - Un enfoque directo, usando una escala de valores de fallas, identificando fallos o eventos potenciales en los procesos operacionales, siendo el resultado: * Una definición de parámetros que influyen en la gravedad de cada fallo. * Una evaluación de los límites de estos parámetros que cambian el nivel de gravedad de los fallos.	**Identificación del contexto:** - **Definir el marco para la gestión del riesgo**, mediante las acciones: Enmarcar el análisis de riesgos, describir el contexto general, delimitar el alcance del estudio, identificar los parámetros a tener en cuenta e identificar las fuentes de amenazas. - **Preparar los indicadores**, a través de: Definir criterios de seguridad, desarrollar una escala de gravedad, desarrollar una gama de niveles de realidad y definir criterios para la gestión del riesgo; para permitir la repetición en el tiempo de las actividades de gestión de riesgos.	**Identificación de activos:** El activo fundamental es la información. Los activos secundarios son: Servicios, aplicaciones informáticas, hardware, redes, instalaciones, personas. Los activos se relacionan de acuerdo a su tipo (S= servicios, D= datos, SW= aplicaciones de software, etc.). **Valoración:** se valoran de acuerdo a su dimensión: disponibilidad, integridad, confidencialidad, autenticidad de los usuarios del servicio,	**Identificación de activos:** Activos tomados en cuenta: información, sistemas, software, hardware y personas. A través de talleres en la organización, hacen preguntas sobre los activos principales, a todos los niveles del personal de la entidad. Luego, con la directiva, usando un cuestionario (worksheet), se identifican y seleccionan los activos más críticos con respecto a los objetivos de la organización (ver apéndice F).

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
ACTIVOS		- Un enfoque organizado y sistemático, con una evaluación automatizada usando el escenario base provisto por la herramienta MEHARI en su base de conocimiento. Los activos son clasificados por su nivel de gravedad y luego son asignados a eventos o incidentes (ver apéndice C).	- **Identificar los bienes (activos principales),** mediante las acciones: identificar los activos críticos, sus relaciones y sus propietarios, identificar los activos de apoyo, sus relaciones y sus propietarios, determinar la relación entre los activos críticos y los activos de apoyo e identificar las medidas de seguridad existentes.	autenticidad del origen de los datos, trazabilidad del servicio, trazabilidad de los datos. Usan los criterios de valoración: Muy alto, alto, medio, bajo y despreciable (ver apéndice E).	Requerimientos de seguridad de los activos: Disponibilidad, integridad y confidencialidad. Describir los requerimientos de seguridad para cada activo crítico. Decidir cuál de los requerimientos de seguridad es más importante para cada activo crítico.

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
AMENAZAS Y VULNERABILIDADES	Utiliza la herramienta del mismo nombre para ejecutar el proceso, usando su base de conocimiento Básicamente las etapas aquí son: - Identificación de amenazas y vulnerabilidades; cálculo de medida del riesgo. - Estudio de vulnerabilidad y amenaza.	Evaluación de la exposición natural, se clasifica en 4 escalas: 1- Muy baja exposición. 2- Baja exposición (apenas expuesto). 3- Exposición media. 4- Exposición alta. Evaluación de los factores disuasivos y preventivos. Evaluación de factores de protección, paliativos y recuperativos. Evaluación de potencialidades, se consideran 5 escalas: *Nivel 0: no considerada*, son escenarios que son tan imposibles que no se incluyen en el conjunto de escenarios a ser analizados.	Usa el módulo 2 y 3 de su proceso y secciones 3 y 4. Todo se realiza por medio de la herramienta EBIOS. Estimar los escenarios de amenazas. - Analizar todos los escenarios. - Evaluar cada uno de los escenarios. **Estudio de las amenazas:** - Fuentes de amenazas: *** Métodos de ataques pertinentes, acciones ilegales, fallas técnicas, compromiso de los datos, desastres naturales, eventos naturales, pérdida de servicios esenciales.	Se identifican. Se valoran en dos sentidos: - **Degradación:** cuán perjudicado resultaría el activo (mide daño causado) - **Frecuencia:** cada cuánto se materializa la amenaza (tasa anual de ocurrencia), siendo valores típicos: 100: muy frecuente (a diario), 10: frecuente (mensual), 1: normal (una vez al año), 1/10: poco frecuente (cada varios años). MAGERIT incorpora el término *vulnerabilidad* por medio de la degradación del activo y la frecuencia de ocurrencia de la amenaza.	Identificar las amenazas para cada activo crítico: *Divulgación, modificación, pérdida/destrucción, interrupción)* **Propiedades de las amenazas:** Activos, actor, motivo (opcional), acceso (opcional) y desenlace. **Fuentes de amenazas:** *Actores humanos usando acceso de redes. *Actores humanos usando acceso físico.. *Problemas del sistema. *Otros problemas (fuera de nuestro control) (ver apéndice F).

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
AMENAZAS Y VULNERABILIDADES		*Nivel 1: Muy poco probable*, la ocurrencia del riesgo es totalmente improbable. *Nivel 2: Improbable*, escenarios que, razonablemente, podría considerarse que nunca podrían ocurrir. *Nivel 3: Probable*, escenarios que podrían ocurrir, en un plazo más o menos corto. *Nivel 4: Muy probable*, el escenario puede ser considerado que sin duda ocurra, y en un tiempo relativamente corto. En el apéndice C se muestra una tabla de vulnerabilidades.	*** Caracterizar los métodos de ataque por los criterios de seguridad que pueden afectar. *** Caracterizar los elementos amenazantes que se asocia con su tipo y causas. *** Agregar un valor que represente el elemento de ataque potencial: 1- accidental o aleatorio, 2- oportunidad o recursos limitados y 3- alto grado de experiencia, oportunidad y recursos. - **Estudio de vulnerabilidades:** *** Identificar las vulnerabilidades de acuerdo con los métodos de ataque *** Estimar eventualmente el nivel de vulnerabilidad.	El libro *"Catálogo de elementos"* presenta una relación de amenazas típicas (ver apéndice E).	**Identificación de amenazas:** Revisar las áreas de interés para activo crítico, usar el perfil de amenaza para identificar amenazas para cada activo crítico. **Identificar Vulnerabilidades** Considerar los siguientes tipos de instrumentos para la identificación: *Escáneres de sistemas operativos. *Escáneres de infraestructura de redes. *Especialidad, escáneres dirigidos o híbridos. *Checklists. *Scripts.

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
AMENAZAS Y VULNERABILIDADES	.		**- Formalización de amenazas:** *** Formular explícitamente las amenazas. *** Priorizar las amenazas en función de su oportunidad. Identificar los criterios de seguridad afectados por métodos de ataques: Disponibilidad, integridad y confidencialidad.		

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
IMPACTO/ RIESGO	Usando la herramienta. Para calcular el riesgo, se basa en una combinación de la valoración de los activos asociados a los activos, y los niveles de amenaza y los niveles de vulnerabilidad que se han obtenido durante la identificación de amenaza y vulnerabilidad. CRAMM determina las medidas de riesgos para: ** Cada activo que se encuentra en un grupo de activos; ** Cada activo que depende de un componente del grupo de activos; ** Cada activo que depende un componente de un	**Evaluación de impacto intrínseco:** la definición de impacto intrínseco de un escenario es la evaluación de la consecuencia del evento de riesgo que está sucediendo actualmente, independientemente de las medidas de seguridad. Consiste en llenar una tabla de impacto intrínseco que trae la herramienta en su base de conocimiento. **Evaluación y reducción del impacto:** Proporciona una evaluación automatizada de impacto, a partir del impacto intrínseco del escenario y los niveles de protección paliativos, y las medidas de recuperación.	A través de la herramienta, hay una lista de impactos, entre los cuales están: incapacidad para prestar el servicio, pérdidas financieras, pérdida de bienes, fondos o valores, pérdida de eficiencia y confianza, etc. Impacto = consecuencia Usa una escala de valores ordinal para determinar el nivel de gravedad de un riesgo. **Identificación del riesgo:** usando la tabla de resumen de los riesgos, amenazas y las necesidades; la formulación de los riesgos incluyen: -El elemento amenazante con sus características, incluyendo su potencial	**Determinar el Impacto:** Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas es directo derivar el impacto que estas tendrían sobre el sistema. ** Impacto acumulado: calculado sobre un activo teniendo en cuenta: a) su valor acumulado (el propio mas el acumulado de los activos que dependen de él). b) las amenazas a las que está expuesto. ** Impacto repercutido: calculado sobre un activo teniendo en cuenta: a) su valor propio.	**Identificación del impacto:** Se definen las descripciones de impacto para los resultados obtenidos de los perfiles de amenazas. Cuando se finaliza la descripción del impacto para un activo crítico, se pasa al siguiente activo y así sucesivamente hasta terminar todos los activos críticos. **Evaluación del impacto de riesgo:** El riesgo es evaluado para proporcionar información adicional para ayudar a los tomadores de decisiones para determinar las prioridades relativas y que riesgo mitigar primero.

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
IMPACTO/ RIESGO	grupo de activos. Las medidas de riesgo para los componentes del grupo de activos son una combinación de los valores de los activos asociados con el activo y los niveles de amenaza y la vulnerabilidad asociada a ese grupo de activos. Las medidas de riesgo de los activos que dependen de un componente del grupo activo es el valor de los activos asociados a dicho activo y los niveles de amenaza y vulnerabilidad determinada por el grupo de activos.	La evaluación se realiza en dos pasos: -Evaluación de un indicador de reducción de impacto. -Evaluación del impacto Finalmente, se define el riesgo global para la organización.	para el ataque, -El método de ataque utilizado por el elemento amenazante, -Las vulnerabilidades explotadas, Las entidades que tienen estas vulnerabilidades, -La oportunidad de la amenaza, -Los requisitos principales de seguridad involucrados, -Repercusiones sobre la organización (en la escala de las necesidades). Se priorizan los riesgos por impacto y amenazas.	b) las amenazas a que están expuestos los activos de los que depende.	OCTAVE sólo evalúa el impacto y no la probabilidad. **Criterios cualitativos para valores de impacto:** alto, medio, bajo. **Áreas de impacto para los criterios de evaluación:** -Reputación/confianza del cliente. -Vida/salud del cliente -Multas/sanciones legales. -Financiero -Otros. Estos criterios son tomados para todos los activos críticos.

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
IMPACTO	.				Finalmente, definir para cada una de las categorías de impacto: bajo, medio o alto impacto. **Evaluación del riesgo:** evaluar el valor de cada impacto a su activo crítico y decidir cuál es el impacto causado para la organización: -Una pérdida alta -Una pérdida media -Una pérdida baja.

Fuente: Autor (2012)

METODOLOGIAS / CRITERIOS	CRAMM	MEHARI	EBIOS	MAGERIT	OCTAVE
SALVAGUARDAS / CONTROLES / MEDIDAS DE SEGURIDAD	Los controles son encontrados en la fase de Gestión de riesgos, mas no en el análisis. La herramienta contiene una biblioteca con más de 3500 contramedidas que se encuentran divididas en grupos, y a su vez en subgrupos. La manera en que una contramedida puede funcionar, es: - Reducir la amenaza, -Reducir la vulnerabilidad, - Reducir el impacto, - Detectar - Recuperar - Transferencia	Paso que realiza fuera del análisis de riesgos. Realiza una evaluación de controles preventivos y correctivos; es decir, para antes y después de que ocurra el riesgo: Factores disuasivos y preventivos. Factores paliativos, de protección y recuperación. También realiza una evaluación de la potencialidad del riesgo, comparando los escenarios encontrados con la lista de escenarios de la base de conocimientos y le otorgan una escala (nivel 0: no considerado, nivel 1: muy improbable, nivel 2: improbable, nivel 3: probablemente, nivel 4: muy probable).	Esta metodología establece los controles fuera del proceso de análisis de riesgos, y lo realiza una vez que ha determinado todos los escenarios de riesgos, la estimación y valoración de los mismos. Es en el módulo 5: estudio de las medidas de seguridad: - Determinar las medidas de seguridad. - Analizar los riesgos residuales - Establecer una declaración de aplicabilidad.	Los controles forman parte de la gestión de los riesgos y los caracteriza: - Procedimientos, o sea, instrucciones paso a paso de qué hay que hacer (preventivos y correctivos) - Política de personal, directrices generales de quién es responsable de cada cosa. - Soluciones técnicas, frecuentes en el entorno de las tecnologías de la información: software, hardware y protección de comunicaciones. Todas las salvaguardas están descritas en detalle en el libro II: Catálogo de elementos (ver apéndice E).	Al igual que el resto de las metodologías, los controles son gestionados en la fase 3: Desarrollo de planes y estrategia de seguridad. Específicamente los planes de seguridad es para mitigar los riesgos en los activos y es a mediano plazo; las estrategias se centra en la mejora de la organización y es a largo plazo; y las listas de dirección de acción son de inmediato.

Fuente: Autor (2012)

Cuadro 9: Ventajas y desventajas de las metodologías CRAMM, MEHARI, EBIOS, MAGERIT Y OCTAVE

METODOLOGÍAS	VENTAJAS	DESVENTAJAS	APORTES AUTOR
CRAMM	• Es una metodología que comprende los procesos de análisis y gestión de riesgos. • Usa un modelo de análisis de riesgos cualitativo y cuantitativo.	• Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad, dejando a un lado el no repudio. • La determinación de los controles para la mitigación de los riesgos la realiza en el proceso de gestión y evaluación de riesgos. • Comprende como elementos del modelo de análisis sólo: activos y dependencias, vulnerabilidades y amenazas. • La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.	• Una metodología de análisis de riesgos debe ser sencilla y de fácil comprensión, tanto para su aplicación como en el mantenimiento, por lo que, debe cumplir un orden cronológico en sus pasos, es decir, debe ser modular. • También, debe ser adaptable para usarse en cualquier entorno. • El principio de no repudio es importante tomarlo en cuenta en el proceso de análisis de riesgos, ya que es una dimensión más de la seguridad de la información y está contemplado en la ley sobre mensajes de datos y firmas electrónicas de nuestro País. • Un análisis de riesgos debe contemplar la determinación de las salvaguardas para los riesgos encontrados.
MEHARI	• Usa un modelo de análisis de riesgos cualitativo y cuantitativo. • Es una metodología para la gestión de riesgos.	• Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad, dejando a un lado el no repudio. • La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión de los riesgos. • La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.	

Fuente: Autor (2012)

Continua

METODOLOGÍAS	VENTAJAS	DESVENTAJAS	APORTES AUTOR
EBIOS	• Comprende los procesos de análisis y gestión de riesgos.	• Está disponible sólo en francés. • Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad, dejando a un lado el no repudio. • No lleva un orden cronológico en el procedimiento de análisis de riesgos. • La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.	• Se debe incorporar la identificación de vulnerabilidades, ya que tienen su importancia relativa en función de la existencia de amenazas reales (factibles), que puedan explotarla y así considerar los controles que mitiguen dichas vulnerabilidades. • Es importante explicar de forma clara y precisa el procedimiento para la identificación de los activos de información.
OCTAVE	• Es una metodología auto dirigida, es decir, la organización gestiona y dirige la evaluación de sus riesgos a través de un equipo multidisciplinario. • Comprende los procesos de análisis y gestión de riesgos. • Involucra a todo el personal de la entidad. • Es la más completa, ya que involucra como elementos de su modelo de análisis: procesos, activos y dependencias, recursos, vulnerabilidades, amenazas y salvaguardas.	• No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. • Usa muchos documentos anexos para llevar a cabo el proceso de análisis de riesgos, lo que la hace tediosa, complicada de entender. • Requiere de profundos conocimientos técnicos. • No explica en forma clara la definición y determinación de los activos de información.	

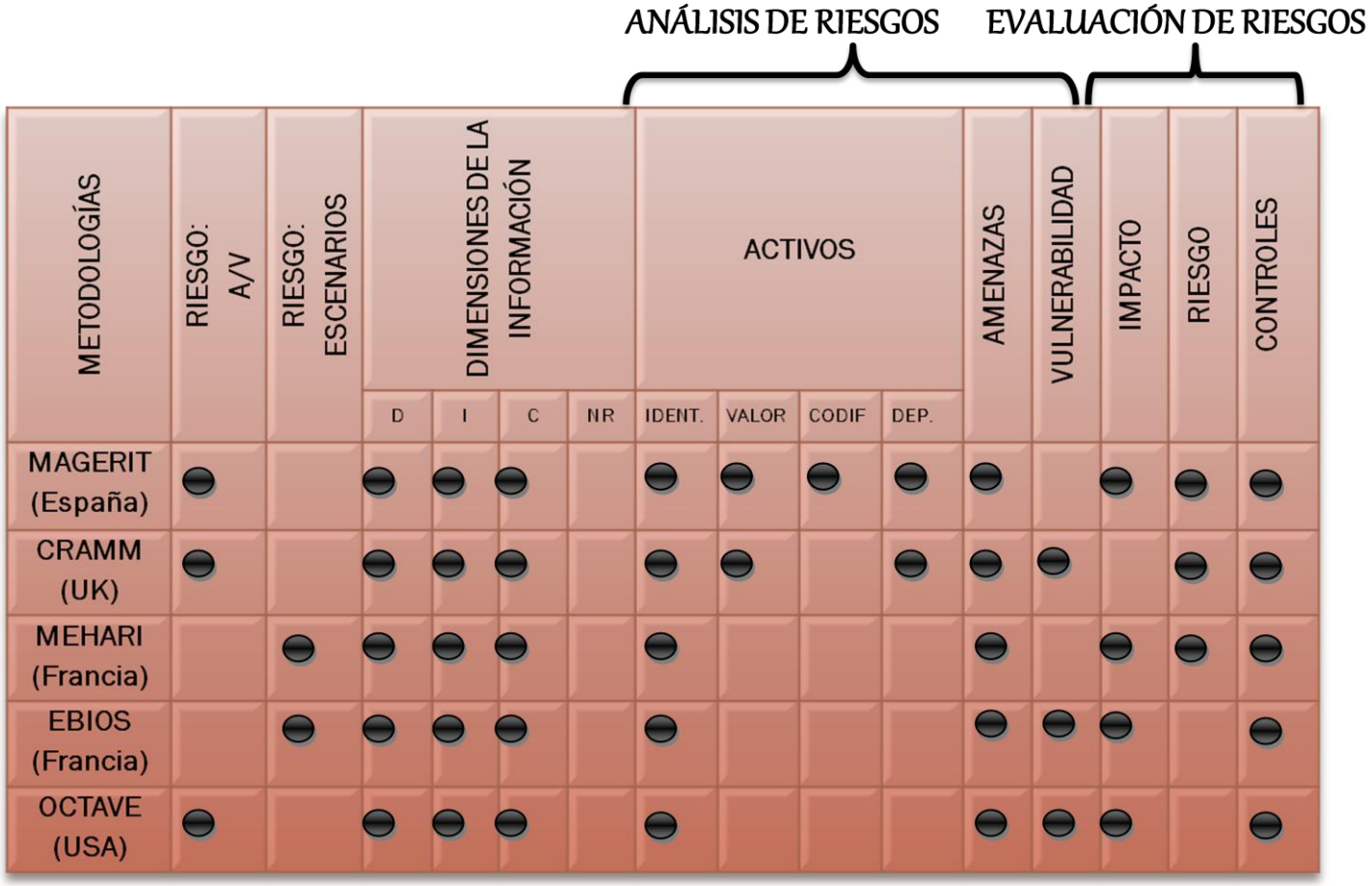
Fuente: Autor (2012)

Continua

METODOLOGÍAS	VENTAJAS	DESVENTAJAS	APORTES AUTOR
MAGERIT	• Es metódica por lo que se hace fácil su comprensión. • Los activos se identifican (tipifican), se buscan sus dependencias, se valoran en cuanto a: disponibilidad, confidencialidad, autenticidad, integridad y trazabilidad. • Comprende los procesos de análisis y gestión de riesgos. • Usa un modelo de análisis de riesgos cualitativo y cuantitativo.	• No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. • No toma en cuenta un análisis de vulnerabilidades. • La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión y evaluación. • Comprende como elementos del modelo de análisis sólo: activos y dependencias, vulnerabilidades y amenazas. • La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos. • El inventario de salvaguardas no está incluido dentro de la metodología sino en la herramienta que la soporta, incluyendo más de 3200 salvaguardas. • Manejo de claves propias que necesitan ser memorizadas para el catálogo de riesgos.	

Fuente: Autor (2012)

Cuadro 10: Resumen comparativo de las metodologías



Fuente: Autor (2012)

CAPITULO V

PROPUESTA: DISEÑO DE UNA METODOLOGIA PARA EL ANALISIS DE RIESGOS EN LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MARISGSI) DE LAS UNIVERSIDADES DE BARQUISIMETO ESTADO LARA

La propuesta tiene como base fundamental proporcionar un método exhaustivo para la optimización de la seguridad de los sistemas de información, detectando las posibles amenazas, vulnerabilidades, estimando los riesgos y el impacto de la información en cualquier institución educativa universitaria por muy pequeñas que estas sean, tanto públicas como privadas.

A continuación se presenta la propuesta metodológica, la cual permite establecer un modelo para realizar el proceso de análisis de riesgos en los SGSI.

METODOLOGIA PARA EL ANALISIS DE RIESGOS EN LOS SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION (MARISGSI) DE LAS UNIVERSIDADES DE BARQUISIMETO ESTADO LARA

INTRODUCCIÓN

MARSGSI se ha elaborado como respuesta a la percepción de que las Instituciones universitarias de Barquisimeto y todo el País, dependen de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio, ya que el uso de los medios informáticos da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

Por otro lado, esta metodología se diseñó principalmente para instituciones universitarias sin importar su tamaño, tanto público como privado, pero es de interés para todos aquellos que trabajen con sistemas de información donde el activo más crítico es la información que manejan dichos sistemas.

Por lo tanto, MARSGSI permite a las entidades conocer el riesgo al que están sometidas y poder analizarlos para mitigarlos, permitiendo a través de un método riguroso obtener conclusiones que permitan tomar decisiones con respecto a los riesgos e impactos. Por lo tanto, se sabe qué puede pasar y se sabe qué hacer cuando pasa.

OBJETIVOS

Concientizar a las instituciones, desde la alta directiva hasta sus empleados y usuarios, sobre la existencia de riesgos en los sistemas de información y la necesidad de controlarlos y afrontarlos.

Brindar una metodología sistemática para analizar dichos riesgos.

Ofrecer una guía para determinar los controles necesarios para mantener los riesgos controlados.

ALCANCE

Esta metodología realiza análisis de los riesgos relacionados con la información contenida en los Sistemas de Gestión de Seguridad de la Información (SGSI), protegiendo las propiedades de disponibilidad, integridad, confidencialidad y no repudio.

En este sentido, MARISGSI se fundamenta en la clausula 8.2 de la norma ISO/IEC 27005:2008 referente al análisis de riesgos: identificación de riesgos y estimación del riesgo; cumpliendo con los indicadores: activos (información), amenazas, vulnerabilidades, impacto y salvaguardas (controles).

CONCIENTIZACION

La concientización es de vital importancia cuando se habla de seguridad de los SGSI, ya que implica la participación y un compromiso claro y bien establecido de la alta dirección o gerencia de las instituciones, debido a que la seguridad de los SGSI está en constante peligro motivado a que las formas de ataque combinan diversos medios para lograr sus objetivos, razón por la cual se debe tomar en cuenta, que no basta solo con implementar soluciones tecnológicas modernas, sino también es importante dar a conocer las políticas de seguridad en las instituciones.

Cabe destacar a las personas como el pilar que hoy hace de los modelos y metodologías de seguridad el desafío más importante, ya que capacitar y crear conciencia suele ser un objetivo muchas veces difícil de alcanzar; por ejemplo, de

nada sirve tener la mejor tecnología de seguridad y los mejores procesos para usarla, si un usuario deja su clave debajo del teclado o en algún lugar visible porque alega que no recordarla.

Por lo tanto, es primordial contar con la participación de todas las personas involucradas en la institución, área o departamento donde se llevará a cabo el proceso de análisis de riesgos, que va desde la alta dirección, gerencia hasta el personal de menor rango. Además, es importante tener presente que los sistemas de seguridad sólo funcionan si:

- Las personas los conocen
- Las personas saben cómo usarlos
- Las personas los aplican.

EQUIPOS DE TRABAJO

Durante el desarrollo del proceso de análisis de riesgos en los SGSI, uno de los factores importantes a tener en cuenta es establecer el equipo de trabajo y sus niveles dentro de la institución, dentro de los cuales se mencionan:

a) **Equipo de dirección:** El perfil necesario para este grupo es de la alta dirección y gerencia, ya que tienen un amplio conocimiento sobre los objetivos estratégicos que se persiguen y la autoridad para aprobar o no cada una de las actividades durante el proceso de análisis. Entre sus responsabilidades se encuentran:
    - Asignar los recursos necesarios para la ejecución del análisis de riesgos.
    - Aprobar los resultados de cada una de las actividades.

b) **Equipo de seguimiento:** conformado por los responsables de las unidades afectadas por el proceso y sus responsabilidades consisten en:
    - Resolver los incidentes que se den durante el análisis.

- Asegurar la disponibilidad de los recursos humanos.
- Aprobar informes de cada actividad.
- Elaborar informes finales para la dirección.

c) **Equipo del proceso:** formado por un grupo multidisciplinario y expertos de distintas áreas a saber: sistemas de información, personal técnico, tecnologías, jurídicos, etc., los cuales dependen de las áreas afectadas en el proceso de análisis; cuyas responsabilidades son:

- Llevar a cabo las tareas o actividades del proceso de análisis.
- Recopilar, procesar y consolidar la información,
- Elaborar reportes.

d) **Director del proceso:** debe ser un directivo de alto nivel, con responsabilidades de seguridad dentro de la institución y sus obligaciones son:

- Dirigir, coordinar y planificar según sea el caso.
- Ser un enlace operacional.

TÉRMINOS Y DEFINICIONES

Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC 27005:2008, p. 9) y que los usuarios legítimos puedan usar la información cuando lo requieran (Daltabuit y otros, 2007, p. 98).

Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos (ISO/IEC 27005:2008, p. 10) y que la información no sea alterada sin autorización (Daltabuit y otros, 2007, p. 98).

Confidencialidad: la información sólo la conozcan quienes tienen derecho a ello (Daltabuit y otros, 2007, p. 97) y la propiedad que esa información esté disponible y

no sea divulgada a personas, entidades o procesos no autorizados (ISO/IEC 27005:2008, p. 10).

No repudio: Proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje u originado o haber sido el destinatario de una acción (Daltabuit y otros, 2007, p. 104).

Activos: recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección (MAGERIT, 2006, p. 17).

Amenazas: es una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio (Stalling, 2004, p. 5).

Vulnerabilidad: la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas (ISO/IEC 27002:2005, p. 16).

También, cualquier debilidad que puede explotarse para causar pérdida o daño al sistema… el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema (Daltabuit y otros, 2007, p. 93).

Riesgo: la posibilidad (la probabilidad) de que se produzca un impacto dado en un activo, es decir, que un agente amenazante explote una vulnerabilidad y provoque un efecto negativo en el sistema (Carracedo, 2004, p. 37).

Salvaguardas (controles): procedimientos o mecanismos tecnológicos que reducen el riesgo (MAGERIT, 2006, p. 25).

Impacto: medida del daño sobre el activo derivado de la materialización de una amenaza (MAGERIT, 2006, p. 23).

Análisis de riesgos: Poderosa herramienta que permite establecer un marco sistemático que provee los indicadores adecuados para llevar acciones de control, mitigación o eliminación de peligros, riesgos e impactos adversos o no deseados en el transcurso de nuestras actividades, cualesquiera que estas sean (Martínez 2002, p. 44).

Estimación del riesgo: proceso para asignar valores a la probabilidad y consecuencias de un riesgo (ISO/IEC 27005:2008, p. 2).

Identificación de riesgo: proceso para encontrar, listar y caracterizar elementos de riesgo (ISO/IEC 27005:2008, p. 2).

ESTRUCTURA DE LA METODOLOGÍA MARISGSI

La metodología MARISGSI está estructurada como sigue:

1) Identificar, valorar y codificar los activos de información
2) Identificar las amenazas de dichos activos
3) Identificar las vulnerabilidades que pueden explotar dichas amenazas.
4) Estimar el impacto que genera el daño causado por las amenazas.
5) Estimar el riesgo que sobre un activo tendría una amenaza.
6) Identificar los controles o salvaguardas para los riesgos causados por las amenazas.

Gráficamente, el proceso de análisis de riesgos de MARISGSI es:

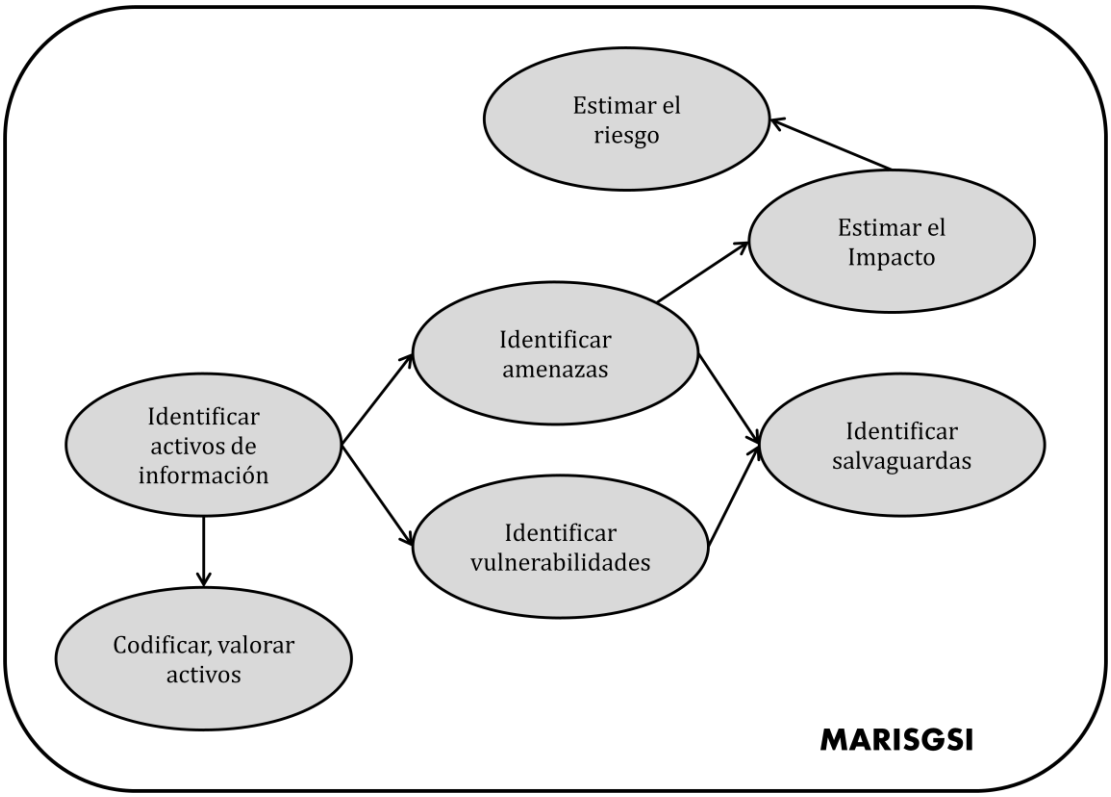


Figura 12: Proceso de análisis de riesgos de la metodología MARISGSI

1) IDENTIFICAR, VALORAR Y CODIFICAR ACTIVOS DE INFORMACIÓN

Identificación de activos:

Una vez que se tiene identificados las funciones y procesos o actividades, se procede a la identificación de los activos, que es esencial para conocer qué debe protegerse para clasificarlos mediante criterios basados en la confidencialidad, integridad, disponibilidad y no repudio de la información. Así, los activos a considerar son:

a) *Información:* archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, procedimientos operacionales o de soporte, planes de continuidad, acuerdos para contingencias, información archivada (papel o electrónico), como ejemplo se pueden mencionar los siguientes: datos personales sensibles, expedientes académicos, matricula de estudiantes, prácticas, publicaciones, titulación, etc.
b) *Sistemas:* sistemas de información que procesan y almacenan información, los cuales son una combinación de activos de software, hardware; por lo que cualquier host, cliente, servidor o red puede ser considerado un sistema, como ejemplos se tienen: sistemas de control de estudios, sistema de evaluación, sistema de inscripciones, etc.
c) *Software:* aplicaciones de software (sistemas operativos, aplicaciones de bases de datos, software de red, aplicaciones de oficina, aplicaciones personalizadas, etc.).
d) *Intangibles:* reputación y la imagen de la entidad.

En este sentido, cada uno de los activos que se identifique debe tener un responsable, que será su propietario[8] y decidirá quién accede y quién no a la información y aplicar medidas de seguridad si existe algún riesgo sobre dicho activo.

Por otro lado, la valoración de los activos viene dada por lo que "vale", no en términos de costo sino por lo que interesa a la institución; es decir, si un activo no puede prescindirse es porque algo vale y es precisamente lo que se desea saber. Por lo que, la valoración se hace con respecto a las dimensiones de confidencialidad, integridad, disponibilidad y no repudio.

a) Disponibilidad: ¿Qué perjuicio causaría no tener o no poder utilizar la información?

[8] El término "Propietario" identifica a la persona o entidad que tiene la responsabilidad gerencial aprobada para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos; no significa que la persona tenga en realidad derechos de propiedad sobre el activo (ISO/IEC 27001:2005, p. 13)

b) Integridad: ¿Qué perjuicio causaría que la información estuviera dañada o corrupta?

c) Confidencialidad: ¿Qué daño causaría que la información la conociera quien no debe?

d) No repudio: ¿Qué daño causaría que la entidad que envía y recibe una información negara ante un tercero el haberla enviado o recibido?

En este sentido, es pertinente realizar una lista con todos los activos identificados, codificados, una breve descripción del mismo, su ubicación y propietario para contar con un inventario completo de lo que se desea proteger, como se muestra en el cuadro siguiente:

Cuadro 11: ACT_ID: Identificación de activos

Activo	Descripción	Codificación	Ubicación	Propietario
Activos (1… N)	Breve descripción del activo	Código	Donde se encuentra	Persona, proceso, entidad, etc.

Fuente: Autor (2012)

Además, se debe documentar los activos como se muestra a continuación:

Cuadro 12: ACT_DOC: Documentación de activos

Activo	Descripción	Clasificación del activo (alto, medio, bajo impacto a la institución)
Activo 1 …….. Activo N	Breve descripción	Indicar que nivel de impacto tiene

Fuente: Autor (2012)

Para el campo **Clasificación del activo**, el equipo de trabajo debe especificar la escala de valoración cuantitativa que se usará para representar a los valores cualitativos: Alto, medio y bajo.

Adicionalmente, para completar la documentación de los activos, se debe llenar el siguiente cuadro con la información pertinente para cada uno de los activos identificados, una vez se hayan identificado las amenazas y las vulnerabilidades; es decir, es el cuadro final que se obtiene del proceso de análisis de riesgos:

Cuadro 13: SAL_ID: Identificación de salvaguardas

ACTIVOS	AMENAZAS ¿Qué es lo que preocupa?	VULNERABILIDAD ¿Cómo puede ocurrir?	NIVEL DE EXPOSICIÓN (A,M,B)	DESCRIPCIÓN DE CONTROLES ACTUALES	DESCRIPCIÓN DE CONTROLES NUEVOS
Activo 1					
Activo n					

Fuente: Autor (2012)

Valoración de los activos:

Una vez determinadas que dimensiones de seguridad interesan de un activo se procede a valorarlo; es decir, se determina el costo que supondría la pérdida de alguna de las dimensiones antes descritas causando un daño sobre el activo; para lo cual hay que definir qué criterios y escalas (cuantitativas, cualitativas o mixtas) se van a usar. De esta manera, la valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la entidad si el activo se ve dañado en dicha dimensión.

En este sentido, los términos típicos utilizados para la valoración cualitativa de los activos incluyen palabras tales como: insignificante, muy bajo, bajo, medio, alto, muy alto, y crítico, donde la elección y extensión de los términos adecuados depende en gran medida de las necesidades de seguridad, tamaño de la institución, y otros factores específicos de la entidad. Con referencia a lo anterior, los posibles criterios utilizados para determinar el valor de un activo incluye su costo original, su costo de

sustitución o re-creación o su valor puede ser abstracto; por ejemplo el valor de la reputación. En este orden de ideas, se lista una serie de criterios a tomar en cuenta para la valoración de los activos según lo establece la norma ISO/IEC 27005:2008 en su anexo B (ver apéndice G):

- Violación de la legislación y/o regulación.
- Efectos negativos en la reputación.
- Violación de la confidencialidad.
- Pérdidas financieras.
- Interrupción del servicio
- Pérdida de credibilidad en el sistema de información interno.
- Daño de la reputación.
- Interrupción del funcionamiento interno.
- Violación de las leyes / regulaciones:
  - ✓ Incapacidad para cumplir las obligaciones legales.
- Incumplimiento de contrato:
  - ✓ Incapacidad para cumplir con las obligaciones contractuales.
- Etc.

Después de establecer los criterios a tener en cuenta, se debe determinar una escala que se usará en toda la institución, para ello se decide cuántos niveles tendrá dicha escala, para lo cual y de acuerdo a la norma ISO/IEC 27005:2008, no existe ninguna regla con respecto al número de niveles que deben usarse. Normalmente, cualquier número de niveles entre 3 (bajo, medio y alto) y 10 pueden ser utilizados siempre que sean consistentes con el enfoque que la entidad este usando para el proceso de evaluación de riesgos.

De esta manera, la institución puede definir sus propios límites para valorar los activos, como "bajo", "medio" o "alto" y deben ser evaluados de acuerdo con los criterios seleccionados (por ejemplo, por una posible pérdida financiera, los límites vienen dados en valores monetarios, pero para consideraciones como poner en peligro

la seguridad personal, la valoración monetaria puede ser compleja). Finalmente, la institución decide lo que es considerado como "bajo", "medio", "alto"; es decir, los límites para la valoración de los activos deben ser determinados por cada institución de acuerdo a sus requerimientos de seguridad (Ver apéndice E).

Por lo tanto, se puede usar la siguiente escala de diez (10) valores para la valoración de los activos identificados:

Cuadro 14: Escala de valoración de activos

VALOR		CRITERIO
10	Muy alto	Daño muy grave a la entidad
7 – 9	Alto	Daño grave a la entidad
4 – 6	Medio	Daño importante a la entidad
1 – 3	Bajo	Daño menor a la entidad
0	Despreciable	Irrelevante a efectos prácticos

Fuente: MAGERIT (2006)

Cabe destacar, que la mayoría de las dimensiones (integridad, confiabilidad, no repudio) permiten una valoración simple, cualitativa o cuantitativa, pero no la disponibilidad; ya que no es lo mismo interrumpir un servicio una hora o un día o un mes, porque detener el servicio una hora puede que sea irrelevante, mientras que un día sin servicio puede causar un daño "moderado", pero un mes puede causar la terminación de la actividad ("muy alto", "crítico"). Por lo tanto, la disponibilidad debe ser valorada usando estructuras más complejas como por ejemplo, un gráfico de escalones, que permita poner en la balanza el valor de toda la entidad frente al costo de las salvaguardas que se deben tomar en cuenta para recuperar la disponibilidad de un activo (MAGERIT, 2006, p. 21). A manera de resumen, en el cuadro siguiente se muestra una relación de las dimensiones para una mejor comprensión en cuanto a la valoración de los activos:

Cuadro 15: Relación de las dimensiones

DISPONIBILIDIAD (D)	INTEGRIDAD (I)
Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados	**Garantía de la exactitud y completitud de la información y los métodos de su procesamiento**
¿Qué importancia tendría que el activo no estuviera disponible?	¿Qué importancia tendría que los datos fueran modificados fuera de control?
• La disponibilidad es una característica que afecta a todo tipo de activos. • La disponibilidad requiere un tratamiento por escalones ya que el costo de la indisponibilidad aumenta de forma no lineal con la duración de una interrupción: desde breves sin importancia, pasando por interrupciones que causan daños considerables hasta llegar a interrupciones que no admiten recuperación de la entidad.	• Los datos tienen alta valoración con respecto a su integridad cuando su alteración voluntaria o intencionada causara grandes daños a la entidad. • Los datos carecen de valor apreciable con respecto a la integridad, cuando su alteración no genera ningún daño.
CONFIDENCIALIDAD (C)	**NO REPUDIO (NR)**
Aseguramiento de que la información es accesible sólo por aquellos autorizados a tener acceso	**Aseguramiento de que cualquier entidad que recibe o envía información no alegue ante terceros que no la envió o recibió**
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?	¿Qué importancia tendría que los datos que se envían o reciben no fueran enviados o recibidos por las entidades correctas?
• Los datos reciben alta valoración con respecto a la confidencialidad cuando su revelación causaría grandes daños a la entidad. • Los datos carecen de un valor apreciable con respecto a la confidencialidad cuando su conocimiento por cualquiera no es preocupante.	• Los datos reciben alta valoración con respecto al no repudio cuando la entidad que recibe o envía alega ante terceros que no envió o no recibió dichos datos.

Fuente: Autor (2012)

Por otro lado, se debe tomar en cuenta la dependencia de los activos, por lo que, la norma ISO/IEC 27005:2008 indica que existen activos que dependen de otros activos para funcionar correctamente; por lo cual, los valores de los activos que dependen de otros pueden ser modificados de la siguiente manera (ver apéndice G):

- ✓ Si los valores de los activos dependientes son inferiores o iguales al valor del activo considerado, su valor sigue siendo el mismo.
- ✓ Si los valores de los activos dependientes es mayor, entonces el valor del activo considerado debe incrementarse de acuerdo con: a) el grado de dependencia y b) los valores de los otros activos.

En síntesis, el proceso para tratar los activos se puede observar de manera gráfica como se indica a continuación:

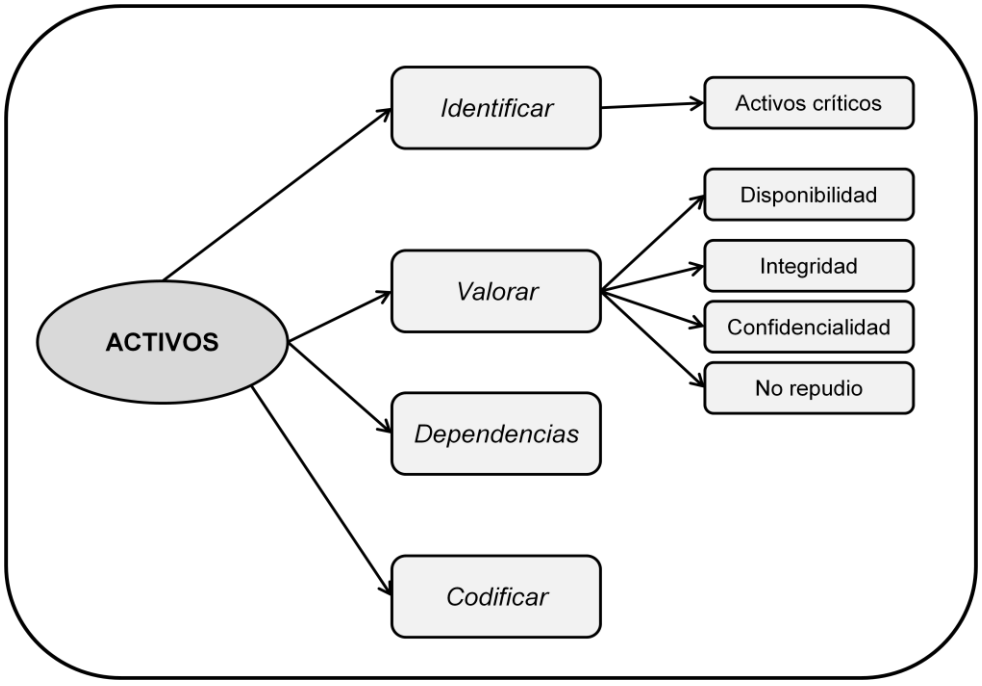


Figura 13: Proceso para los activos
Fuente: Autor (2012)

2) IDENTIFICAR AMENAZAS

Este paso tiene como objetivo identificar y recopilar una lista de las fuentes de amenazas (algunos ejemplos se presentan en el cuadro 12) potenciales aplicables a los SGSI. En este sentido, una fuente de amenaza es cualquier circunstancia o acontecimiento con el potencial para causar daño a los activos tales como la información, los procesos y sistemas y por lo tanto las organizaciones, éstas pueden ser de origen natural o humano, y podrían ser accidentales o deliberadas. Es así, que las personas es la fuente principal de amenazas en un ataque a un activo, por lo que en el cuadro siguiente se indican algunas de estas:

Cuadro 16: Amenazas comunes relacionadas con personas

Amenaza	Motivación	Acción de la amenaza
Hacker	Robo de información	Hacking, ingeniería social, intrusiones al sistema.
Criminal de computación	Destrucción de la información Ganancia monetaria Alteración de datos no autorizado	Crímenes computacionales, actos fraudulentos (duplicación, robo de identidad), soborno de información.
Terrorista	Destrucción Explotación	Bomba/terrorismo Guerra de la información Ataque al sistema
Espionaje industrial (compañías, gobiernos vecinos y otros)	Ventaja competitiva Espionaje económico	Chantaje, robo de información, violación de la privacidad, acceso no autorizado al sistema.
Empleados	Curiosidad Ganancia monetaria Errores no intencionales	Asalto a información Fraude Robo información confidencial

Fuente: Autor (2012)

Además, las amenazas pueden surgir desde dentro o desde fuera de la entidad y pueden afectar a más de un activo. En tal caso, pueden causar impactos diferentes en función de que activos se vean afectados, y cada fuente de amenaza puede estar asociada a un riesgo diferente.

Cabe destacar, que no todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir; así cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cantidad; en el apéndice H se muestra el anexo C de la norma ISO/IEC 27005:2008 que muestra una tabla de ejemplos de amenazas típicas.

Cuadro 17: Lista parcial de amenazas y sus fuentes

AMENAZAS/FUENTES	DESCRIPCION
Divulgación accidental	Revelación accidental o no autorizada de información clasificada, personal o sensible
Alteración de software	La modificación, inserción o borrado intencional del sistema operativo o los programas de aplicación, por usuarios autorizados o no, comprometen la confidencialidad, integridad, disponibilidad y no repudio de los datos, programas o recursos controlados por el sistema. Esto incluye código malicioso, como bombas lógicas, caballos de troya, puertas traseras y virus.
Uso de banda ancha	El uso accidental o intencionado del uso de las comunicaciones de banda ancha para otros fines.
Alteración intencional de los datos	La modificación, inserción o borrado intencional de datos, por usuarios autorizados o no, comprometen la disponibilidad, confidencialidad, integridad y no repudio de los datos producidos, procesados, controlados o almacenados por los sistemas de procesamiento de datos.
Error de configuración del sistema (accidental)	Un error de configuración accidental durante la instalación inicial o actualización de hardware, software, equipos de comunicación o entorno operacional.
Interrupción / fallas de las telecomunicaciones	Cualquier enlace de comunicaciones, unidad o componente falla lo suficiente para causar interrupción en la transferencia de datos vía telecomunicaciones entre terminales de computadoras, procesadores remotos o distribuidos e instalaciones anfitrión.

Fuente: Autor (2012)

En conclusión, este proceso de identificación consiste en obtener una lista de las amenazas con la identificación del tipo y sus fuentes. Además, gráficamente se puede representar tal como se indica en la siguiente figura:

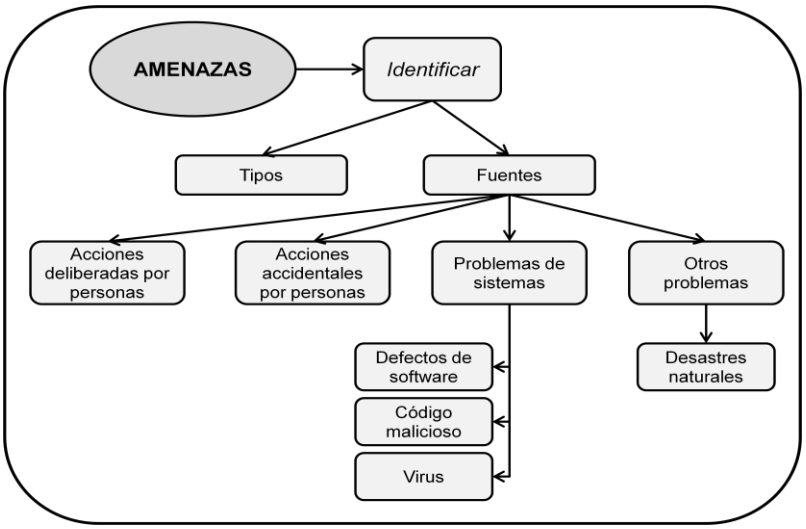


Figura 14: Proceso para las amenazas
Fuente: Autor (2012)

3) IDENTIFICAR VULNERABILIDADES

La vulnerabilidad es un defecto o debilidad dentro del procedimiento de seguridad del sistema, diseño, implementación o de los controles internos; por lo que identificadas las amenazas que pueden perjudicar a los activos, hay que estimar qué tan vulnerables son y esto se hace tomando en cuenta la:

a) *Degradación:* qué tan perjudicado resultaría el activo, es decir, mide el daño causado por un incidente en el supuesto caso de que ocurriera y frecuentemente se caracteriza como una fracción del valor del activo, por lo que se suelen escuchar expresiones como "totalmente degradado" o "degradado en una pequeña fracción".

b) *Frecuencia:* cada cuánto tiempo se materializa la amenaza y coloca en perspectiva la degradación, ya que ésta puede ocasionar terribles consecuencias pero puede ser muy improbable que se materialice, mientras que otra amenaza puede ser de bajas consecuencias pero tan frecuente como para terminar acumulando un daño considerable al

activo. Por lo tanto, la frecuencia es representada como una tasa anual de ocurrencia, tal como se muestra en el siguiente cuadro:

Cuadro 18: Valores referenciales de frecuencia

Valor	Frecuencia	Frecuencia de ocurrencia
100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años

Fuente: MAGERIT V.2 (2006)

A continuación, se presenta un cuadro de referencia entre la frecuencia y la degradación:

Cuadro 19: Referencia de frecuencia y degradación

DEGRADACION (Daño causado)	*ALTO*	Impacto moderado	Impacto alto	Impacto alto	Impacto alto
	MEDIO	Impacto bajo	Impacto moderado	Impacto alto	Impacto alto
	BAJO	Impacto bajo	Bajo impacto	Impacto moderado	Impacto alto
NIVEL DE IMPACTO		Poco frecuente	Normal	Frecuente	Muy frecuente
		VALOR DE FRECUENCIA			

Fuente: Autor (2012)

Como resultado de este paso, se obtiene una lista de vulnerabilidades de los activos ya identificados (defectos o debilidades) que podrían ser explotadas por las fuentes de amenazas potenciales, tal como se muestra en el cuadro siguiente:

Cuadro 20: VUL_ID: Identificación de amenazas y vulnerabilidades

ACTIVOS	AMENAZAS (¿Qué es lo que preocupa?)	VULNERABILIDADES (¿Cómo puede ocurrir?)	NIVEL DE EXPOSICIÓN (A, M, B)
Activo 1			
Activo 2			
……			
Activo n			

Leyenda: A = Alto, M = Medio, B = Bajo
Fuente: Autor (2012)

Finalmente, el proceso para la identificación de vulnerabilidades se puede representar gráficamente como se indica en la siguiente figura:

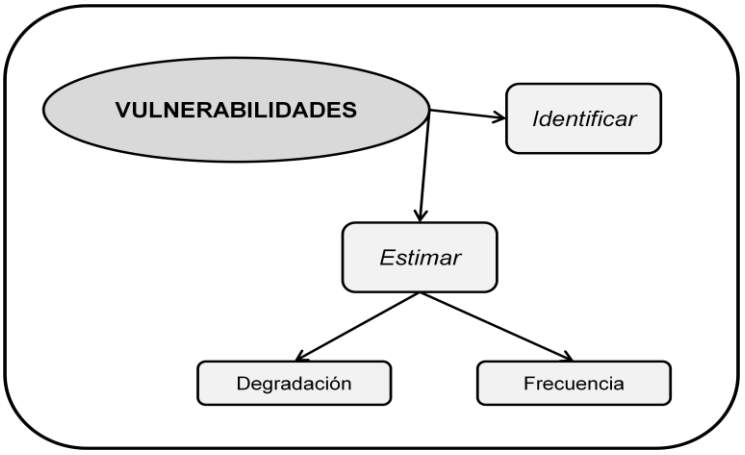


Figura 15: Proceso para las vulnerabilidades
Fuente: Autor (2012)

4) ESTIMAR IMPACTO

Impacto es la estimación del grado de daño o de la pérdida que podría ocurrir en la institución y las consecuencias se refieren al daño total, no únicamente a los impactos a corto plazo o inmediatos, cuantas más severas sean las consecuencias de la amenaza, mayor es el riesgo relacionado al sistema y por lo tanto a la entidad.

Por otro lado, para comprender mejor el impacto, MAGERIT (2006) lo define como "la medida del daño sobre el activo derivado de la materialización de una amenaza" (p. 23).

En este sentido, para determinar el impacto de un activo se pueden considerar múltiples factores, por ejemplo, para establecer el valor de un "servidor de base de datos" no sólo basta con calcular o estimar el valor que representa la información para la institución, sino también qué tanto influye en la operación de la misma, además de todos los costos inherentes como son costo de hardware, software (licencias de uso), instalación y mantenimiento del mismo.

Por lo tanto, para la estimación del impacto sobre los activos identificados se recomienda completar el siguiente cuadro:

Cuadro 21: EST_IMP: Determinación del impacto

ACTIVO / FACTOR	FACTOR 1	FACTOR 2	FACTOR ……	FACTOR N	IMPACTO A LA ENTIDAD	IMPACTO
Activo 1						
Activo 2						
Activo …						
Activo N						
				IMPACTO TOTAL		

Fuente: Autor (2012)

Donde:

- **Activo:** Nombre del activo

- **Impacto a la entidad:** este valor es tomado del cuadro 13: documentación de los activos, nivel de exposición (Alto, Medio, Bajo), usando la siguiente escala numérica para representar el impacto: Alto = 10, Medio = 5, Bajo = 2.
- **Impacto:** resultado total de la suma de los factores multiplicado por el valor del impacto a la entidad.

Además, al inicio del proceso de análisis de riesgos, el equipo de trabajo debe indicar la escala de valoración que va a tener cada uno de los factores que influyen en la determinación del impacto final de cada uno de los activos ya identificados. Dicha escala, tendrá valores cuantitativos para realizar el cálculo final del impacto; así como se muestra en el siguiente cuadro de valoración de factores:

Cuadro 22: VAL_FAC: Valoración de factores

Nº FACTOR	FACTOR	VALORACIÓN (Alto, Medio, Bajo)
1	**Factor 1**	
2	**Factor 2**	
n	**Factor n**	

Fuente: Autor (2012)

Cuadro 23: EST_IMP: Determinación del impacto

ACTIVO / FACTOR	FACTOR 1	FACTOR 2	FACTOR 3	FACTOR 4	IMPACTO A LA ENTIDAD	IMPACTO
Contratos de docentes		5		2	10	70
Red de datos	5	5	10	2	10	220
				IMPACTO TOTAL		290

Fuente: Autor (2012)

5) IDENTIFICAR LOS CONTROLES O SALVAGUARDAS

Los controles incluyen características de seguridad, restricciones propuestas por la gerencia, seguridad del personal, seguridad de estructuras, de áreas y de dispositivos físicos.

Por lo tanto, un control es cualquier acción, dispositivo, procedimiento, técnica o alguna medida que reduce la vulnerabilidad de un sistema a una amenaza. El análisis de los controles debe incluir una investigación de la eficacia de las medidas de seguridad existentes, también se debe identificar los nuevos controles que se podrían poner en ejecución en el sistema.

Finalmente, ya con todos los datos anteriores se procede a completar el siguiente cuadro de información incluyendo los controles existentes y nuevos para cada uno de los activos identificados anteriormente:

Cuadro 24: Análisis de riesgos

ACTIVOS	AMENAZAS ¿Qué es lo que preocupa?	VULNERABILIDAD ¿Cómo puede ocurrir?	NIVEL DE EXPOSICIÓN (A,M,B)	DESCRIPCIÓN DE CONTROLES ACTUALES	DESCRIPCIÓN DE CONTROLES NUEVOS
Activo 1					
Activo 2					
…….					
Activo n					

Fuente: Autor (2012)

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La investigación permitió concluir que las instituciones universitarias de Barquisimeto:

- ✓ Carecen en su totalidad de Sistemas de Gestión de Seguridad de la Información (SGSI), por lo que desconocen el estándar ISO/IEC 27001:2005 que proporciona un modelo para establecer, implementar, operar, monitorear, revisar y mejorar un SGSI.
- ✓ No estandarizan la seguridad de la información; es decir, no implementan las normas ISO/IEC 27002:2005 e ISO/IEC 27005:2008 concernientes a la gestión de los riesgos de información.
- ✓ No tienen identificados, inventariados ni codificados sus activos de información más críticos; es decir, aquellos activos que son vulnerables y generan riesgos para las instituciones.
- ✓ No realizan procedimientos para identificar amenazas y vulnerabilidades en los activos de información de sus sistemas; es por esto, que su gestión de seguridad se basa en corregir a través de experiencias pasadas y empíricas, los fallos que se van presentando.
- ✓ No existen bitácoras referentes a amenazas y vulnerabilidades presentadas en sus activos de información, lo que les permite estimar los impactos causados a la institución.

- ✓ No establecen controles de acuerdo a la normativa para mitigar los riesgos presentados.
- ✓ Carecen de procedimientos de seguridad que les permitan mantener controlados y gestionados los riesgos que ocasionan las amenazas en los activos de información.
- ✓ No tienen conocimiento sobre las variadas metodologías existentes para realizar el proceso de análisis de riesgos en SGSI.
- ✓ En su totalidad, los entrevistados mostraron gran interés en contar con una metodología para realizar el proceso de análisis de riesgos en sus sistemas que sea sencilla de operar y aplicar.

En relación a la comparación de las metodologías CRAMM, EBIOS, MEHARI, MAGERIT y OCTAVE; se concluye que todas las metodologías no incluyen en su proceso de análisis de riesgos, la dimensión de no repudio de la información cuando se valoran los activos de la entidad. Además, el análisis de riesgos contempla solo la identificación de los activos críticos, identificación de amenazas y vulnerabilidades; mientras que la estimación del impacto, del riesgo y la determinación de los controles para minimizar los riesgos lo realizan en un proceso aparte llamado Evaluación de riesgos. Con respecto a los activos, la metodología MAGERIT es la única que los identifica, valora, codifica y obtiene las dependencias de los mismos; mientras que el resto de las metodologías sólo los identifica.

Finalmente, la metodología MARISGSI dispone de un procedimiento para identificar y codificar los activos críticos de una entidad, así como valorarlos con respecto a sus dimensiones incluyendo el no repudio; también, se realiza una identificación de las amenazas, sus fuentes y las vulnerabilidades a las que se encuentran expuestos los activos críticos identificados; y de esta manera, estimar el impacto y el riesgo para establecer los controles necesarios y pertinentes para minimizar dichos riesgos.

Recomendaciones

En base a las conclusiones obtenidas en este estudio, se recomienda:

1) Implementar Sistemas de Gestión de Seguridad de la Información (SGSI) en concordancia con las necesidades, objetivos, requerimientos de seguridad, procesos empleados, tamaño y estructura de cada institución.
2) Una vez implementados los SGSI y usando la metodología MARISGSI, realizar el proceso de análisis de riesgos a los activos de información más críticos, de manera tal que se identifiquen las amenazas y vulnerabilidades de dichos activos, valorando los riesgos a los que se encuentran expuestas las instituciones para finalmente estimar el impacto generado y así establecer y aplicar los controles necesarios para mitigar los riesgos encontrados.

BIBLIOGRAFIA

Aceituno, V. (2006). *Information Security Management Maturity Model*. ISM3. ISECOM.

Alberts, C. y Dorofree, A. (2003). *Managing information security risk.* Pearson Education. Boston.

Arias, F. (1997). *El proyecto de investigación.* Caracas: Episteme.

Carracedo G. J. (2004). *Seguridad en redes telemáticas.* McGraw Hill. España

Daltabuit, E., Hernández, L, Mallén, G. y Vásquez, J. (2007). *La seguridad de la Información.* Editorial LIMUSA S.A. Grupo Noriega editores. México.

De Freitas, V. (2009). *Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar.* Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento, 6 (1), 43-55.

Giménez, M. (2008). *La importancia de la seguridad de la información en las empresas*. [Artículo en línea]. Boletín semanal Caracas Digital. Disponible en: http://www.caracasdigital.com/noticias-masdetalle.php?detalle=795. [Consulta: 2010, Febrero 01].

Hernández, S., Fernández, C. y Baptista, L. (2006). *Metodología de la investigación.* McGraw Hill. Cuarta Edición. México.

ISO/IEC 27001:2005. (2005). *Tecnología de la información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos.*

ISO/IEC 27002:2005. (2005). *Tecnología de la información-Técnicas de seguridad-Código para la práctica de la gestión de la seguridad de la información.*

ISO27K. 2010. [Página web en línea]. Disponible en: http://www.iso27001security.com. [Consulta: Marzo 22, 2010].

Kerlinger, F. y Lee, H. (2002). *Investigación del comportamiento.* 4º Edición. McGraw Hill. México.

Martínez Ponce de León, J. (2002). *Introducción al análisis de riesgos*. Editorial Limusa. D.F, México.

Mendoza, R. (2010). *Sistema de gestión para la seguridad de la información, caso: centro de tecnología de información y comunicación del Decanato de Ciencias y*

Tecnología – UCLA. Tesis de maestría. Universidad Centroccidental Lisandro Alvarado. Barquisimeto Estado Lara.

Real Academia Española (RAE). (2001). *Diccionario de la lengua Española.* Edición 22. Madrid, España.

Royal, F. (1998). *Seguridad en los sistemas informáticos.* Ediciones Díaz de Santos, S.A. Madrid, España.

Sabino, C. (1992). *El proceso de investigación.* Caracas: PANAPO.

Stracuzzi, S. y Pestana, F. (2004). *Metodología de la investigación cuantitativa.* FEDUPEL. Caracas, Venezuela.

UPEL Universidad Pedagógica Experimental Libertador. (2006). *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales.* FEDUPEL. Caracas, Venezuela.

Zapata, O. (2006). *Herramientas para elaborar tesis e investigaciones socioeducativas.* Editorial Pax México. México.

APÉNDICE A: INSTRUMENTO CUESTIONARIO

UNIVERSIDAD CENTROCCIDENTAL LISANDRO ALVARADO
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO – DCyT

CUESTIONARIO

Fecha: _____/_____/_____

Unidad o Departamento: _____

Universidad: _____

Use la siguiente escala para valorar su opinión con respecto a cada ítem presentado:

Categoría	**Codificación (Valor asignado)**
Definitivamente Sí	5
Probablemente Sí	4
Indeciso	3
Probablemente No	2
Definitivamente No	1

Marque con una "equis" (X) según corresponda.

Responda todos los ítems con sinceridad, su información es de vital importancia y tendrá carácter confidencial.

Gracias por su aporte.

Ítems	Enunciado	1	2	3	4	5
1	¿Cree que los servicios ofrecidos por los sistemas de información en la Institución, están disponibles para sus usuarios cuando ellos así lo requieran?					
2	¿En los últimos 5 años, la información disponible en los sistemas de información de la institución, ha sido divulgada, robada, mal utilizada o saboteada?					
3	¿Considera que la institución implementa estrategias de seguridad que cubran los procesos donde la información es el activo principal?					
4	¿Considera que la institución tiene codificados los activos principales de sus Sistemas de Gestión de la Seguridad de Información (SGSI)?					
5	¿El personal de la institución conoce las políticas de seguridad manejadas para sus SGSI?					
6	¿La institución ha resuelto satisfactoriamente las amenazas presentadas en los últimos 5 años, en sus SGSI?					
7	¿Tiene conocimiento de la existencia del código de buenas prácticas para la gestión de la seguridad de la información (Estándar ISO/IEC 27002:2005?					
8	¿Conoce el estándar ISO/IEC 27001:2005, que proporciona los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI?					
9	¿La información de los SGSI de la institución, es accedida por personas no autorizadas?					
10	¿Se aplican los requerimientos especificados en el estándar ISO/IEC 27001:2005 en los SGSI de la institución?					
11	¿Dentro de la documentación importante que maneja la institución, existe el documento de la norma ISO/IEC 27001:2005?					
12	¿En los últimos 5 años la institución ha manejado algún procedimiento para analizar los riesgos presentados en sus SGSI?					
13	¿Considera que los activos principales de los SGSI se encuentran protegidos contra posibles amenazas?					
14	¿Cree Ud. que el principio de No repudio de la información forma parte de la seguridad que maneja la institución en sus SGSI?					
15	¿En los últimos 5 años, algún activo de los SGSI ha sido vulnerado?					

Ítems	Enunciado	1	2	3	4	5
16	¿Considera importante que la institución cuente con un procedimiento para realizar el análisis de riesgos a los SGSI?					
17	¿La institución lleva un registro de las vulnerabilidades que se han presentado en los SGSI en los últimos 5 años?					
18	¿La institución tiene identificados y registrados los activos principales de los SGSI?					
19	¿Se tiene claramente identificados los riesgos a los que están expuestos los activos de los SGSI?					
20	¿Se lleva un registro de las amenazas que se han detectado en los últimos 5 años en los activos de los SGSI?					
21	¿Se ha estimado el impacto que tendría en la institución, la falta de existencia de un proceso de análisis de riesgos a los SGSI?					
22	¿Se usa algún método definido para determinar el impacto que causa una amenaza a los activos de los SGSI de la institución?					
23	¿Tiene conocimiento sobre cuáles son los objetivos de control especificados en el estándar ISO/IEC 27002:2005, que usa la institución para la seguridad de la información?					
24	¿Conoce algún caso, en los últimos 5 años, donde la información que manejan los SGSI de la institución haya sido copiada por personas no autorizadas?					
25	¿Se han reportado casos donde la información contenida en los SGSI de la institución, ha sido borrada o modificada sin autorización en los últimos 5 años?					
26	¿Se han implementado técnicas de seguridad para garantizar la integridad de la información de los SGSI?					
27	¿Se han implementado técnicas de seguridad para garantizar que la información de los SGSI solo pueda ser accedida por las partes autorizadas?					
28	¿La institución carece de políticas de seguridad que ofrezcan la disponibilidad de sus servicios de los SGSI?					
29	¿La institución evalúa el grado en que pueden ser afectados sus activos por las amenazas identificadas?					
30	¿La institución ha usado procedimientos, normas, estándares, para resolver satisfactoriamente los peligros que acechan a los SGSI?					
31	¿Se desconoce la norma ISO/IEC 27001:2005 para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI?					

Ítems	Enunciado	1	2	3	4	5
32	¿Existe una supervisión en el uso de la norma ISO/IEC 27002:2005, que permita el incremento de la calidad operativa de la institución?					
33	¿La institución prevé los riesgos reales de los SGSI permitiendo la aplicación funcional de la norma ISO/IEC 27005:2008?					
34	¿La institución toma medidas de protección (salvaguardas) sobre sus activos?					
35	¿La institución toma en cuenta el principio de No repudio de la información, como parte de la seguridad de los SGSI?					
36	¿El histórico de los casos relacionados con vulnerabilidades de los SGSI de la institución en los últimos 5 años, se encuentra debidamente archivado?					
37	¿La institución carece de mecanismos o salvaguardas para la protección de sus activos?					
38	¿La carencia de los principios de seguridad de la información permite identificar los riesgos presentes en los SGSI?					
39	¿La aplicación de los procedimientos de seguridad prevén el impacto de posibles riesgos en los SGSI?					

APÉNDICE B: INSTRUMENTO **ENTREVISTA**

UNIVERSIDAD CENTROCCIDENTAL LISANDRO ALVARADO
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO – DCyT

ENTREVISTA

Datos del entrevistado

Apellidos y Nombres: _____

Cargo: _____

Departamento: _____

Universidad: _____

La presente entrevista tiene como objetivo obtener información de índole confidencial que solo será usada para diagnosticar la necesidad de contar con una Metodología para el análisis de Riesgos en los Sistemas de Gestión de Seguridad de la Información (SGSI) en las Universidades del Estado Lara.

Se le agradece responder con sinceridad cada ítem de la entrevista.

1. ¿Describa cuáles son los activos principales que posee la institución. Están protegidos?

   _____

   _____

   _____

2. ¿Indique la frecuencia con que se presentan las amenazas en los activos de los Sistemas de Gestión de Seguridad de la Información (SGSI). Describa esas amenazas?

_____

_____

3. ¿Describa las vulnerabilidades que han presentado los SGSI en la institución en los últimos 5 años. Con qué frecuencia se presentan?

_____

_____

_____

4. ¿Cuenta la institución con un manual de políticas de seguridad vigentes para mantener seguros sus SGSI, con qué frecuencia lo aplica?

_____

_____

_____

5. ¿Describa cuales de los SGSI que maneja la institución son más vulnerables y por qué?

_____

_____

_____

6. ¿Explique cuál es el procedimiento que realizan cuando un SGSI es afectado por alguna amenaza?

_____

_____

_____

7. ¿Realiza la institución un Análisis de Riesgos a sus SGSI? Explique cómo lo hace.

_____

_____

_____

_____

_____

_____

8. ¿Cuándo se han presentado los riesgos en los SGSI, se ha determinado que salvaguardas (controles) hay dispuestos y cuan eficaces son frente a esos riesgos. Explique?

   _____

   _____

   _____

   _____

9. ¿Están todos los activos principales claramente inventariados, De qué manera?

   _____

   _____

   _____

   _____

10. ¿En los últimos 5 años, se han identificado los impactos que han tenido las pérdidas de confidencialidad, integridad, disponibilidad y no repudio sobre los activos de la institución?

    _____

    _____

    _____

    _____

11. ¿La institución usa algún procedimiento para realizar el análisis de riesgos a los SGSI? ¿Cuál?

    _____

    _____

    _____

    _____

12. Existe una bitácora de recomendaciones sobre los análisis de vulnerabilidades realizado en la institución en los últimos 5 años?

    _____

    _____

    _____

13. ¿En los últimos 5 años, se ha realizado algún proceso para calcular la magnitud de los riesgos, explique?

    _____
    _____
    _____
    _____

14. ¿Cree que los servicios ofrecidos por los sistemas de información en la Institución, están disponibles para sus usuarios cuando ellos así lo requieran, explique?

    _____
    _____
    _____
    _____

15. ¿En los últimos 5 años, se ha realizado un análisis de vulnerabilidades de sus SGSI. Cuál fue el resultado?

    _____
    _____
    _____
    _____

16. ¿La mayoría de las amenazas presentadas en los SGSI de la institución han sido solucionadas a través de algún procedimiento de análisis de riesgos. Explique el procedimiento aplicado?

    _____
    _____
    _____
    _____
    _____
    _____
    _____

17. ¿Aplica la institución la norma ISO/IEC 27001:2005 para mantener seguros sus SGSI, explique?

    _____

    _____

    _____

18. ¿Se han presentado situaciones en los últimos 5 años, donde se han eliminado activos debido al alto impacto que éstos provocan sobre la misión de la institución?

    _____

    _____

    _____

    _____

    _____

19. ¿Se aplica el estándar ISO/IEC 27005:2008 para el análisis de riesgos en los SGSI, explique cómo?

    _____

    _____

    _____

    _____

    _____

20. ¿Considera que los activos principales de los SGSI se encuentran protegidos contra posibles amenazas, explique cómo?

    _____

    _____

    _____

    _____

21. ¿Conoce cuáles son las metodologías existentes en el mercado para realizar el análisis de riesgos a los SGSI? Explique.

    _____

    _____

22. ¿Implementan alguna de las metodologías existentes en el mercado para el análisis de riesgos en la institución. Indique cuál?

    _____

    _____

    _____

23. ¿Considera necesario diseñar una Metodología para el análisis de riesgos en los SGSI de la institución para mitigar o corregir los riesgos en los SGSI. Explique por qué?

    _____

    _____

    _____

24. ¿La institución aplica la norma ISO/IEC 27002:2005 como guía para la gestión de la seguridad de la información. Explique?

    _____

    _____

    _____

25. ¿La institución tiene identificados y registrados los activos principales de los SGSI. Cómo?

    _____

    _____

    _____

26. ¿En los últimos 5 años, la información disponible en los sistemas de información de la institución, ha sido divulgada, robada, mal utilizada o saboteada?

    _____

    _____

27. ¿Considera que el principio de No repudio de la información forma parte de la seguridad que maneja la institución en sus SGSI, explique?

    _____

    _____

    _____

28. ¿Se han reportado casos donde la información contenida en los SGSI de la institución, ha sido borrada o modificada sin autorización en los últimos 5 años, explique?

    _____

    _____

29. ¿Se tiene claro el nivel de riesgo que tienen los activos de los SGSI de la institución, explique?

    _____

    _____

    _____

30. ¿Describa los controles aplicados a los SGSI para reducir la exposición al riesgo protegiendo los activos principales de la institución?

    _____

    _____

31. ¿En los últimos 5 años, los controles usados para reducir los riesgos en los SGSI han sido correctivos o preventivos, explique?

    _____

    _____

Gracias por su colaboración

APÉNDICE C: TABLAS DE LA BASE DE CONOCIMIENTOS DE LA METODOLOGÍA MEHARI

MEHARI™ 2010 - release 2-2

Mehari 2010 knowledge base

Worksheet	Objective		
Intro	Description and pointers within the worksheets of the file. If the security policy of your organisation forbids the use of macros, it will not be possible to use the masks below.		
Nav	Scheme of navigation within the knowledge base		
License	Reminder of the public licence of MEHARI		
Stakes analysis and asset classification module.		Classification tables: T1, T2, T3 & Classif	Mask ➔ ☐
T1, T2 and T3	Classification tables		
Classif	Asset classification		
Security services diagnostic module (or Audit)		Questionnaires: from 01Org to 14 ISM + Themes & ISO 27002 scoring	Mask ➔ ☐
Domain 01 Org to 14 ISM	Questionnaires relative to MEHARI security domains (01 to 14)		
Services	Recap of the quality of the security services		
Themes	MEHARI security themes		
ISO 27002	ISO 27002 scoring table following the diagnostic of MEHARI security services		
Risk analysis module (identification, assessment and classification of risks)		Risk analysis: Events, Risks per asset or event	Mask ➔ ☐
Expo	Table of natural likelihood of threats (or natural exposure)		
Scenarios	Table of risk scenarios including formulas for risk assessment		
Risk%Asset	Display of seriousness for the scenarios based on the asset involved		
Risk%event	Display fo the seriousness of scenarios based on the origin or event considered		
Risk treatment : options, risk reduction plans and follow on		Risk treatment: ActionPlans, Obj_PA, Obj_Projects	Mask ➔ ☐
Action_plans	Risk reduction plans selected		
Obj_PA	Tab used for the selection of risk reduction plans		
Obj_Projects	Tab used for the selection of risk reduction projects		
Parameters and permanent elements of the method		Grids for risk acceptability, Impact and Likelyhood evaluation	Mask ➔ ☐
Vulnerabilities	This tab and the following are provided by the method		
Seriousness	Seriousness Table function on Impact and Likelihood		
IP Grids	Impact and Likelihood tables for the scenarios		

You can use the forum www.**mehari.info** to post questions, remarks or comments

Translation managed by
Jean-Louis Roule
Jean-Philippe Jouas

Date	Revision status and comments
October 2010	Edition 2-1
April 2011	Edition 2-2 Edition of a few formulas in ISO scoring and IP grids

Methods space

Club de la Sécurité de l'Information Français
11, rue de Mogador, 75009 PARIS
T : +33 1 53 25 08 80 / F : +33 1 53 25 08 88
http://www.clusif.asso.fr/

Escenarios por tipo de activos y nivel de gravedad

Number of scenarios per asset type and seriousness level		Availability					Integrity					Confidentiality				
Data and information assets		S. 1	S. 2	S. 3	S. 4		S. 1	S. 2	S. 3	S. 4		S. 1	S. 2	S. 3	S. 4	
Data and information																
D01	Data files and data bases accessed by applications	0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D02	Shared office files and data	0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D03	Personal office files (on user work stations and equipments)	0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D04	Written or printed information and data kept by users and personal archives	0	0	0	0	>						0	0	0	0	>
D05	Listings or printed documents											0	0	0	0	>
D06	Exchanged messages, screen views, data individually sensitive	0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D07	electronic mailing	0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D08	(Post) Mails and faxes	0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D09	Patrimonial archives or documents used as proofs	0	0	0	0	>						0	0	0	0	>
D10	IT related Archives	0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D11	Data and information published on public or internal sites	0	0	0	0	>	0	0	0	0	>					
Service assets																
General Services																
G01	User workspace and environment	0	0	0	0	>										
G02	Telecommunication Services (voice, fax, audio & videoconferencing, etc.)	0	0	0	0	>	0	0	0	0	>					
IT and networking Services																
R01	Extended Network Service	0	0	0	0	>	0	0	0	0	>					
R02	Local Area Network Service	0	0	0	0	>	0	0	0	0	>					
S01	Services provided by applications	0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
S02	Shared Office Services (servers, document management, shared printers, etc.)	0	0	0	0	>	0	0	0	0	>					
S03	Users' disposal of Equipments (workstations, local printers, peripherals, specific interfaces, etc.)	0	0	0	0	>										
S04	Common Services, working environment: messaging, archiving, print, editing, etc.	0	0	0	0	>	0	0	0	0	>					
S05	Web editing Service (internal or public)	0	0	0	0	>	0	0	0	0	>					
Management process types of assets		**Efficiency**														
Management processes for compliance to law or regulations																
C01	Compliance to law or regulations relative to personal information protection	0	0	0	0	>										
C02	Compliance to law or regulations relative to financial communication	0	0	0	0	>										
C03	Compliance to law or regulations relative to digital accounting control	0	0	0	0	>										
C04	Compliance to law or regulations relative to intellectual property	0	0	0	0	>										
C05	Compliance to law or regulations relative to the protection of information systems	0	0	0	0	>										
C06	Compliance to law or regulations relative to people safety and protection of environment	0	0	0	0	>										

Números de escenarios por tipo de evento y nivel de gravedad

Number of scenarios sorted per type of event and seriousness level				Number of scenarios for each seriousness level			
Type	*Code type*	*Event*	*Code*	*S. 1*	*S. 2*	*S. 3*	*S. 4*
Absence of personnel, accidental	AB.P	Absence of personnel from a partner	AB.P.Pep	0	0	0	0
		Absence of internal personnel	AB.P.Per	0	0	0	0
Absence or unavailability of service, by accident	AB.S	Absence of service : Power supply	AB.S.Ene	0	0	0	0
		Absence of service : Air-conditioning	AB.S.Cli	0	0	0	0
		Absence of service : Premises	AB.S.Loc	0	0	0	0
		Absence or unavailability of application maintenance	AB.S.Maa	0	0	0	0
		Absence or unavailability of system maintenance	AB.S.Mas	0	0	0	0
Serious accident affecting the environment	AC.E	Lightning	AC.E.Fou	0	0	0	0
		Fire	AC.E.Inc	0	0	0	0
		Flooding	AC.E.Ino	0	0	0	0
Accident affecting hardware	AC.M	Breakdown of computing or telecommunication equipment	AC.M.Equ	0	0	0	0
		Breakdown of auxiliary equipment	AC.M.Ser	0	0	0	0
Voluntary absence of personnel	AV.P	Social conflict with strike	AV.P.Gre	0	0	0	0
Design error	ER.L	Blocking bug due to a design or programming error (internal development)	ER.L.Lin	0	0	0	0
Error affecting hardware or originated by personnel	ER.P	Loss or oblivion of document or media	ER.P.Peo	0	0	0	0
		Error of operation or execution of a procedure	ER.P.Pro	0	0	0	0
		Capture or typing error	ER.P.Prs	0	0	0	0
Incident caused by the environment	IC.E	Damage due to obsolescence	IC.E.Age	0	0	0	0
		Water damage	IC.E.De	0	0	0	0
		Electrical overloading	IC.E.Pol	0	0	0	0
		Damage due to pollution	IC.E.Se	0	0	0	0
Incident or dysfunction of software	IF.L	Production incident	IF.L.Exp	0	0	0	0
		Blocking bug in system or packaged software	IF.L.Lsp	0	0	0	0
		Blocking jam due to external cause (worm)	IF.L.Ver	0	0	0	0
		Virus	IF.L.Vir	0	0	0	0
Malevolence effected using logical or functional means	MA.L	Attempt to block an account	MA.L.Blo	0	0	0	0
		Deliberate erasure or massive pollution of system configurations	MA.L.Cfg	0	0	0	0
		Deliberate erasure of physical or logical media	MA.L.Del	0	0	0	0
		Electromagnetic harnessing	MA.L.Ele	0	0	0	0
		Logical alteration of data or functions)	MA.L.Fal	0	0	0	0
		Forgery (of messages or data)	MA.L.Fau	0	0	0	0
		Replay of transaction	MA.L.Rej	0	0	0	0
		Malicious saturation of computer equipments or networks	MA.L.Sam	0	0	0	0
		Complete destruction of data (files and backup copies)	MA.L.Tot	0	0	0	0
		Harnessing of files or data (illegal remote loading or copy)	MA.L.Vol	0	0	0	0
Malevolence effected using physical means	MA.P	Rigging or alteration of hardware equipment	MA.P.Fal	0	0	0	0
		Terrorism	MA.P.Ter	0	0	0	0
		Vandalism	MA.P.Van	0	0	0	0
		Robbery	MA.P.Vol	0	0	0	0
Non compliance of procedures	PR.N	Inadequate procedures	PR.N.Api	0	0	0	0
		Procedures not applied due to lack of resources	PR.N.Naa	0	0	0	0
		Procedures not applied due to ignorance	PR.N.Nam	0	0	0	0
		Procedures not applied deliberately	PR.N.Nav	0	0	0	0

Escalas de impacto

MEHARI 2010 standard scales for impact and likelihood levels

Scale of impact

Level 4: Vital

At this level, the impact is very serious, and even the existence and survival of the entity (or at least one of its main activities) is in danger.

Should the organization survive such a malfunction, there would be serious and durable consequences.

Level 3: Very Serious

The impact is considered very serious at the level of the entity, although its future would not be at risk.

In financial terms, this would have a seriously negative impact on the profits for the period, although there would not be a massive pull-out by shareholders.

In terms of public image, this level of malfunction often damages the organization's reputation to such an extent that it would take several months to restore it, even if the financial impact cannot be precisely evaluated.

Accidents that lead to months of organizational disorder for an enterprise would also be evaluated at this level.

Level 2: Serious

Malfunctions at this level would have a clear impact on the entity's operations, results or image, but are globally manageable.

Level 1: Not significant

At this level, any resulting damage would have no significant impact on the results or image of the entity, even if some staff members were deeply involved in re-establishing the original status

Lista de vulnerabilidades

List of intrinsic vulnerabilities							
	Type of supporting asset	*Type of damage*	*Type of vulnerability*	*Criteria AICE*	*Code*	*Selection*	*Comments*
Category: Service							
	Software Configuration	Alteration	Possibility of alteration of software configurations (software and parameters)	A and I	Cfl.alt	1	
		Failure	Possibility of software failure (bug)	A	Cfl.bug	1	
		Disclosure of software	Possibility of disclosure of a software file	C	Cfl.dif	1	
		Erasure	Possibility of erasure of software configurations	A	Cfl.eff	1	
		Unauthorized use	Possibility of denial to use (due to lack of license)	I	Cfl.lic	1	
		Pollution	Possibility of pollution of software configurations	I	Cfl.pol	1	
	Account or means to access the service	Lock	Possibility of user accounts to be blocked	A	Cpt.blo	1	
		Loss	Possibility of loss of capability to connect to the service	A	Cpt.dis	1	
	Hardware (Equipment)	Destruction	Possibility of destruction of equipment	A	Eq.des	1	
		Failure	Possibility of failure of equipment	A	Eq.hs	1	
		Not operable	Possibility of non operable equipment	A	Eq.mo	1	
	Premises	Unavailability	Possibility of premises to be not accessible	A	Loc.ina	1	
	Media containing software	Destruction	Possibility of destruction of media containing software	A	Med.des	1	
		Loss	Possibility of loss of media containing software	A	Med.dis	1	
		Exchange	Possibility of loss of media containing software	I	Med.ech	1	
		Not operable	Possibility of non operable media containing software	A	Med.ine	1	
	Auxiliary means or equipments	Unavailability	Possibility of unavailability of auxiliary means or equipments	I	Ser.hs	1	
Category: data							
	means to access data	Loss	Possibility of loss of means allowing to access data (physical or logical keys)	A	Cle.dis	1	
	Data in transit, messages, screens	Alteration	Possibility of alteration of data in transit or messages	I	Dtr.alt	1	
		Disclosure	Possibility of duplication and disclosure of data in transit, messages, screens	C	Dtr.div	1	
		Loss	Possibility of loss of data in transit or messages	A and C	Dtr.per	1	
	File containing data	Alteration	Possibility of alteration of files containing data	I	Fic.alt	1	
		Disclosure	Possibility of duplication or diffusion (and disclosure) of a file containing data	C	Fic.dif	1	
		Erasure	Possibility of erasure of data files	A	Fic.eff	1	
		Pollution	Possibility of pollution (slow evolution) of data in a file	A	Fic.pol	1	
	Media containing data	Destruction	Possibility of destruction of media containing data	A	Med.des	1	
		Loss	Possibility of loss of media containing data	A and C	Med.dis	1	
		Duplication	Possibility of duplication and disclosure of media containing data	A and C	Med.dup	1	
		Exchange	Possibility of exchange of media containing data	A and C	Med.ech	1	
		Unavailability	Possibility of unavailability of media containing data	A	Med.ine	1	
Category: management process							
	Procedures and instructions	Inefficiency	Possibility that procedures observed be inefficient (towards laws, regulations or contractual commitments)	E	Pro.inf	1	

APÉNDICE D : BASE DE CONOCIMIENTO DE LA METODOLOGIA EBIOS

PREMIER MINISTRE
Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS

BASES DE CONNAISSANCES

Version du 25 janvier 2010

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 65 - Fax 01 71 75 84 90

Fuentes de amenazas

3 Types de sources de menaces

Les sources de menaces représentent une typologie des choses ou personnes à l'origine des risques.

On distingue les sources par :
- leur origine humaine ou non humaine,
- leur facilité d'accès au sujet de l'étude (interne ou externe),
- dans le cas de sources humaines :
  - leur caractère intentionnel ou accidentel,
  - leurs capacités (force intrinsèque, selon leurs ressources, expertise, dangerosité…),
- dans le cas de sources non humaines :
  - leur type (naturelle, animale, contingence…).

Chaque type de source de menace fait l'objet d'exemples, qui figurent en *italique*.

Sources humaines agissant de manière délibérée

Personnes ou groupes de personnes mal intentionnées, qu'elles soient physiques ou morales, et qui peuvent être à l'origine de risques. Elles peuvent être internes ou externes au sujet de l'étude. Leurs capacités (force intrinsèque) dépendent principalement de leurs ressources, de leur expertise et du temps qu'elles peuvent accorder. Leur motivation peut être le jeu, la cupidité, la vengeance, une idéologie, le chantage, l'égo, la recherche d'un avantage concurrentiel, le terrorisme…

Source humaine interne, malveillante, avec de faibles capacités

Collaborateur malveillant avec des possibilités d'action limitées sur le système d'information (personnel en fin de contrat ou voulant se venger de son employeur ou de ses collègues…), stagiaire agissant de manière ludique, client désirant obtenir des avantages, personnel d'entretien.

Source humaine interne, malveillante, avec des capacités importantes

Collaborateur malveillant avec d'importantes connaissances et possibilités d'action sur le système d'information (manager ambitieux en fin de contrat ou voulant se venger de son employeur ou de ses collègues, développeur agissant par égo ou de manière ludique, fraudeur, actionnaires…), sous-traitant ou prestataire, personnel de maintenance ou d'assistance à distance.

Source humaine interne, malveillante, avec des capacités illimitées

Collaborateur malveillant avec des connaissances et possibilités d'action illimitées sur le système d'information (administrateur système ou réseau agissant par vengeance, dirigeant…).

Source humaine externe, malveillante, avec de faibles capacités

Script-kiddies, vandale.

Source humaine externe, malveillante, avec des capacités importantes

Militant agissant de manière idéologique ou politique, pirate passionné, casseur ou fraudeur, ancien employé désirant se venger d'un licenciement, concurrent, groupement professionnel, organisation de lobbying, syndicat, journaliste, organisation non gouvernementale.

Source humaine externe, malveillante, avec des capacités illimitées

Organisation criminelle, agence gouvernementale ou organisation sous le contrôle d'un État étranger, espions, organisation terroriste.

Amenazas y vulnerabilidades

4 Menaces et vulnérabilités génériques

Les menaces génériques représentent les incidents ou les sinistres types qui peuvent affecter les biens supports.

Elles peuvent être classées selon :

- le type de biens supports sur lequel elles portent (MAT, LOG, CAN, PER) ;
- le critère de sécurité des biens essentiels qu'elles sont susceptibles d'affecter (disponibilité, intégrité, confidentialité) ;
- leur mode opératoire :
  - les détournements d'usages (USG) : les biens supports sont détournés de leur cadre d'utilisation nominal (usage des fonctionnalités possibles, prévues ou autorisées) sans être modifiés ni endommagés ;
  - l'espionnage (ESP) : les biens supports sont observés, avec ou sans équipement supplémentaire, sans être endommagés ;
  - les dépassements de limites de fonctionnement (DEP) : les biens supports sont surchargés ou utilisés au-delà de leurs limites de fonctionnement ;
  - les détériorations (DET) : les biens supports sont endommagés, partiellement ou totalement, temporairement ou définitivement ;
  - les modifications (MOD) : les biens supports sont transformés ;
  - les pertes de propriété (PTE) : les biens supports sont aliénés (perdus, volés, vendus, donnés…), sans être modifiés ni endommagés, de telle sorte qu'il n'est plus possible d'exercer les droits de propriété.

Chaque menace générique fait l'objet d'une description et d'exemples, qui figurent en *italique*. Les critères de sécurité directement concernés, les principales vulnérabilités exploitables et les pré-requis pour la source de menace complètent la description.

La correspondance entre la typologie précédente et la présente typologie est présentée en annexe.

Concernant les principales vulnérabilités exploitables, celles-ci représentent les caractéristiques génériques des biens supports qui peuvent être exploitées pour que les menaces puissent se réaliser. Elles ne sont pas exhaustives et devraient systématiquement être adaptées pour être intelligibles pour les personnes à qui elles sont destinées et que leur niveau de détail soit approprié au sujet étudié et à l'objectif poursuivi.

Amenazas lógicas

Menaces sur les logiciels

M7. LOG-USG – Détournement de l'usage prévu d'un logiciel

Les fonctionnalités du logiciel sont utilisées, sans le modifier ni l'endommager, pour réaliser des actions autres que celles prévues.

Lecture ou copie inappropriée via un logiciel : lecture ou copie de données de configuration ou de données métiers, fouille de contenu stocké, collecte de données métiers partagées.

Suppression inappropriée via un logiciel : effacement d'enregistrements, de fichiers ou de répertoires, qu'ils soient sur une mémoire, un disque dur ou un support, effacement de traces de journaux d'événements, effacement de fichiers ou de répertoires partagés sur un réseau.

Création ou modification inappropriée via un logiciel : saisie de messages ne respectant pas la charte d'utilisation d'un espace d'échange non modéré (forum, blog…), élévation de privilèges d'un compte utilisateur, modification du contenu ou du nom de fichiers ou de répertoires, partagés ou non, ou de la configuration d'un système, qu'ils soient sur une mémoire, un disque dur ou un support (insertion d'une page web sur un site Internet, défiguration de site Internet, élévation de privilèges, modification des traces de journaux d'événements, fraude…), croisement d'informations dont le résultat est confidentiel, utilisation de canaux cachés pour traiter ou véhiculer des données discrètement (stéganographie).

Usage inapproprié de fonctionnalités d'un logiciel : usage d'un logiciel professionnel pour des besoins personnels, détournement de fonctionnalités de réseaux (envoi massif d'informations par courrier électronique – spam, envoi de données ou de fichiers partagés, détournement de services d'un réseau…), utilisation de logiciels contrefaits ou copiés.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

Principales vulnérabilités exploitables :
- Donne accès à des données
- Permet de manipuler des données (supprimer, modifier, déplacer…)
- Peut être détourné de son usage nominal (offre la possibilité d'envois massifs…)
- Permet d'utiliser des fonctionnalités avancées

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du logiciel
- Accès logique au logiciel (franchissement légitime ou non, ou contournement)

M8. LOG-ESP – Analyse d'un logiciel

Le logiciel est analysé (code source, fonctionnement, fonctionnalités…), sans être endommagé, depuis l'intérieur ou l'extérieur du système d'information. Des données et du savoir faire peuvent ainsi être compromis.

Collecte de données de configuration d'un réseau, balayage d'adresses réseau ou de ports, observation des caractéristiques de fonctionnement d'un logiciel (observation de l'espace mémoire d'un logiciel depuis un débogueur, ingénierie inverse…).

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :
- Accessibilité et intelligibilité du code source
- Possibilité d'observer le fonctionnement du logiciel

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du logiciel
- Accès logique au logiciel (franchissement légitime ou non, ou contournement)

Amenazas de personas

Menaces sur les personnes

M19. PER-USG – Dissipation de l'activité d'une personne

Les ressources de la personne sont employées à faire autre chose que ce qu'elle devrait faire, sans la faire changer ni l'affecter physiquement. Ses performances peuvent ainsi être diminuées.

Exploitation du temps de travail (réception et tri ou lecture de pourriel – spam, retransmission d'un canular – hoax, retransmission d'une escroquerie – scam…), exploitation d'une personne en dehors de ses prérogatives ou détournement des services rendus par une personne (utilisation illégitime des ressources d'une personne par d'autres services, travail en dehors des missions fixées dans un contrat…), blocage de l'accès d'une personne à son lieu de travail (occupation, grève, squattage, manifestation, routes coupées suite à des inondations, pandémie, zone de guerre, manifestations sur la route d'accès ou blocage du site, zone interdite pour cause de contamination bactérienne, utilisation de locaux à d'autres fins que celles prévues…).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Sujet à la dissipation (distraction, difficulté à cadrer ses activités…)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation de la personne
- Établissement d'une relation (hiérarchique, professionnelle, d'autorité, personnelle, sociale…) avec la personne

M20. PER-ESP – Espionnage d'une personne à distance

Observation ou écoute d'une personne, avec ou sans équipement d'amplification sensorielle ou de capture, depuis l'intérieur ou l'extérieur des locaux, sans être affectée physiquement.

Divulgation involontaire, observation du comportement et des habitudes.

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :
- Peu discret (loquace, sans réserve…)
- Routinier (habitudes facilitant l'espionnage récurrent)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation de la personne
- Proximité physique de la personne

Medidas de seguridad

5 Mesures de sécurité génériques

Mesures de sécurité issues du [RGS]

Les mesures suivantes proviennent des chapitres du [RGS] intégrant des clauses qui peuvent être interprétées comme des mesures de sécurité. Les lignes de défense auxquelles elles contribuent ont été déterminées.

2. Un cadre pour gérer la sécurité des systèmes d'information

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Réou.
2.2. Six grands principes de gestion de la SSI	2.2.1.	Adopter une démarche globale	Voir [RGS]	X	X	X
2.2. Six grands principes de gestion de la SSI	2.2.2.	Adapter la SSI selon les enjeux	Voir [RGS]	X	X	X
2.2. Six grands principes de gestion de la SSI	2.2.3.	Gérer les risques SSI	Voir [RGS]	X	X	X
2.2. Six grands principes de gestion de la SSI	2.2.4.	Élaborer une politique SSI	Voir [RGS]	X	X	X
2.2. Six grands principes de gestion de la SSI	2.2.5.	Utiliser les produits et prestataires labellisés SSI	Voir [RGS]	X	X	
2.2. Six grands principes de gestion de la SSI	2.2.6.	Viser une amélioration continue	Voir [RGS]	X	X	X
2.3. Intégration de la SSI dans le cycle de vie des systèmes d'information	2.3.1.	Des efforts proportionnés aux enjeux SSI	Voir [RGS]	X	X	X
2.3. Intégration de la SSI dans le cycle de vie des systèmes d'information	2.3.2.	Un engagement systématique : l'homologation de sécurité	Voir [RGS]	X	X	X
2.3. Intégration de la SSI dans le cycle de vie des systèmes d'information	2.3.3.	Des outils ciblés pour les projets de système d'information	Voir [RGS]	X	X	X

3. Fonctions de sécurité

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Réou.
3.2. Authentification	3.2.1.	Utilisation de mécanismes cryptographiques	Voir [RGS]	X	X	
3.2. Authentification	3.2.2.	Utilisation des identifiants / mots de passe statiques	Voir [RGS]	X	X	
3.2. Authentification	3.2.3.	Authentification d'une personne par certificat électronique	Voir [RGS]	X	X	
3.2. Authentification	3.2.4.	Authentification d'un serveur par certificat électronique	Voir [RGS]	X	X	
3.3. Signature électronique	3.3.1.	Utilisation de mécanismes cryptographiques	Voir [RGS]	X	X	
3.3. Signature électronique	3.3.2.	Signature d'une personne par certificat électronique	Voir [RGS]	X	X	X
3.3. Signature électronique	3.3.3.	Cachet d'un serveur par certificat électronique	Voir [RGS]	X	X	X
3.4. Confidentialité	3.4.1.	Utilisation de mécanismes cryptographiques	Voir [RGS]	X	X	
3.4. Confidentialité	3.4.2.	Confidentialité par certificat électronique	Voir [RGS]	X	X	
3.4. Confidentialité	3.4.3.	Habilitations	Voir [RGS]	X		

Medias de seguridad: control de acceso

11. Contrôle d'accès

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
11.1. Exigences métier relatives au contrôle d'accès	11.1.1.	Politique de contrôle d'accès	Il convient d'établir, de documenter et de réexaminer une politique de contrôle d'accès sur la base des exigences d'exploitation et de sécurité.	X	X	
11.2. Gestion de l'accès utilisateur	11.2.1.	Enregistrement des utilisateurs	Il convient de définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information.	X		
11.2. Gestion de l'accès utilisateur	11.2.2.	Gestion des privilèges	Il convient de restreindre et de contrôler l'attribution et l'utilisation des privilèges.	X	X	
11.2. Gestion de l'accès utilisateur	11.2.3.	Gestion du mot de passe utilisateur	Il convient que l'attribution de mots de passe soit réalisée dans le cadre d'un processus formel.		X	
11.2. Gestion de l'accès utilisateur	11.2.4.	Réexamen des droits d'accès utilisateurs	Il convient que la direction revoie les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel.	X	X	
11.3. Responsabilités utilisateurs	11.3.1.	Utilisation du mot de passe	Il convient de demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	X	X	
11.3. Responsabilités utilisateurs	11.3.2.	Matériel utilisateur laissé sans surveillance	Il convient que les utilisateurs s'assurent que tout matériel laissé sans surveillance est doté d'un dispositif de protection approprié.	X	X	
11.3. Responsabilités utilisateurs	11.3.3.	Politique du bureau propre et de l'écran vide	Il convient d'adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information.	X	X	
11.4. Contrôle d'accès au réseau	11.4.1.	Politique relative à l'utilisation des services en réseau	Il convient que les utilisateurs aient uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.	X	X	
11.4. Contrôle d'accès au réseau	11.4.2.	Authentification de l'utilisateur pour les connexions externes	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X	
11.4. Contrôle d'accès au réseau	11.4.3.	Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques.	X	X	
11.4. Contrôle d'accès au réseau	11.4.4.	Protection des ports de diagnostic et de configuration à distance	Il convient de contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	X	X	
11.4. Contrôle d'accès au réseau	11.4.5.	Cloisonnement des réseaux	Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient séparés sur le réseau.	X	X	
11.4. Contrôle d'accès au réseau	11.4.6.	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, il convient de restreindre la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	X	X	
11.4. Contrôle d'accès au réseau	11.4.7.	Contrôle du routage réseau	Il convient de mettre en oeuvre des mesures du routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	X	X	
11.5. Contrôle d'accès au système d'exploitation	11.5.1.	Ouverture de sessions sécurisées	Il convient que l'accès aux systèmes d'exploitation soit soumis à une procédure sécurisée d'ouverture de session.	X	X	
11.5. Contrôle d'accès au système d'exploitation	11.5.2.	Identification et authentification de l'utilisateur	Il convient d'attribuer à chaque utilisateur un identifiant unique et exclusif et de choisir une technique d'authentification permettant de vérifier l'identité déclarée par l'utilisateur.	X	X	
11.5. Contrôle d'accès au système d'exploitation	11.5.3.	Système de gestion des mots de passe	Il convient que les systèmes qui gèrent les mots de passe soient interactifs et fournissent des mots de passe de qualité.	X	X	
11.5. Contrôle d'accès au système d'exploitation	11.5.4.	Emploi des utilitaires système	Il convient de limiter et de contrôler étroitement l'emploi des programmes utilitaires permettant de contourner les mesures d'un système ou d'une application.		X	
11.5. Contrôle d'accès au système d'exploitation	11.5.5.	Déconnexion automatique des sessions inactives	Il convient que les sessions inactives soient déconnectées après une période d'inactivité définie.	X	X	X
11.5. Contrôle d'accès au système d'exploitation	11.5.6.	Limitation du temps de connexion	Il convient de restreindre les temps de connexion afin d'apporter un niveau de sécurité supplémentaire aux applications à haut risque.	X		
11.6. Contrôle d'accès aux applications et à l'information	11.6.1.	Restriction d'accès à l'information	Pour les utilisateurs et le personnel chargé de l'assistance technique, il convient de restreindre l'accès aux informations et aux fonctions applicatives conformément à la politique de contrôle d'accès.	X	X	

Annexes

Correspondance entre les nouvelles menaces et celles d'EBIOSv2

Le tableau suivant montre que les méthodes d'attaque de la méthode EBIOSv2 sont parfaitement prises en compte dans les menaces génériques des présentes bases de connaissances.

Nouvelles menaces / Méthodes d'attaque EBIOSv2	M1. MAT-USG	M2. MAT-ESP	M3. MAT-DEP	M4. MAT-DET	M5. MAT-MOD	M6. MAT-PTE	M7. LOG-USG	M8. LOG-ESP	M9. LOG-DEP	M10. LOG-DET	M11. LOG-MOD	M12. LOG-PTE	M13. RSX-USG	M14. RSX-ESP	M15. RSX-DEP	M16. RSX-DET	M17. RSX-MOD	M18. RSX-PTE	M19. PER-USG	M20. PER-ESP	M21. PER-DEP	M22. PER-DET	M23. PER-MOD	M24. PER-PTE	M25. PAP-USG	M26. PAP-ESP	M27. PAP-DET	M28. PAP-PTE	M29. CAN-USG	M30. CAN-ESP	M31. CAN-DEP	M32. CAN-DET	M33. CAN-MOD	M34. CAN-PTE
1. Incendie				X												X						X					X							
2. Dégâts des eaux				X												X			X								X							
3. Pollution				X																		X					X							
4. Sinistre majeur				X												X						X					X							
5. Destruction de matériels ou de supports				X																							X							
6. Phénomène climatique			X	X											X	X					X	X					X							
7. Phénomène sismique				X												X			X			X					X							
8. Phénomène volcanique				X												X			X			X					X							
9. Phénomène météorologique			X	X											X	X			X		X	X					X							
10. Crue				X												X			X			X					X							
11. Défaillance de la climatisation			X																		X													
12. Perte d'alimentation énergétique			X																															
13. Perte des moyens de télécommunication													X		X	X	X	X																
14. Rayonnements électromagnétiques			X																															
15. Rayonnements thermiques			X																		X													
16. Impulsions électromagnétiques				X																														
17. Interception de signaux parasites compromettants		X												X																				
18. Espionnage à distance		X												X						X						X				X				
19. Ecoute passive														X																X				

APÉNDICE E: LIBRO II MAGERIT: CATÁLOGO DE ELEMENTOS

MINISTERIO DE
ADMINISTRACIONES
PÚBLICAS

MAGERIT – versión 2

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

II - Catálogo de Elementos

Madrid, 20 de junio de 2006
NIPO 326-05-047-X
Catálogo general de publicaciones oficiales
http://publicaciones.administracion.es

Criterios de valoración de los activos

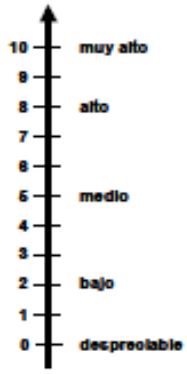
4. Criterios de valoración

Para valorar los activos vale, teóricamente, cualquier escala de valores. A efectos prácticos es sin embargo muy importante que

- se use una escala común para todas las dimensiones, permitiéndo comparar riesgos,
- se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas[3] y
- se use un criterio homogéneo que permita comparar análisis realizados por separado

Si la valoración es económica, hay poco más que hablar; pero frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos.

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle, se puede optar por la tabla simplificada de 5 niveles. Ambas escalas, detallada y simplificada se correlacionan como se indica a continuación:



valor		*criterio*
10	muy alto	daño muy grave a la organización
7-9	alto	daño grave a la organización
4-6	medio	daño importante a la organización
1-3	bajo	daño menor a la organización
0	despreciable	irrelevante a efectos prácticos

La tabla siguiente pretende guiar con más detalle a los usuarios valorando de forma homogénea activos cuyo valor es importante por diferentes motivos, habiéndose tomado en consideración los siguientes:

- seguridad de las personas
  - información de carácter personal[4]
- obligaciones derivadas de la ley, del marco regulatorio, de contratos, etc.
- capacidad para la persecución de delitos
- intereses comerciales y económicos
- pérdidas financieras
- interrupción del servicio

3 Así siempre es igual de relevante que un activo sea el doble de valioso que otro, independientemente de su valor absoluto. Por el contrario, sería extraño opinar que un activo vale dos más que otro sin explicitar su valor absoluto pues no es igual de relevante pasar de 0,1 a 2,1, que pasar de 1.000.000 a 1.000.002.

4 La información de carácter personal se califica por dos vías: administrativa y valorada. La vía administrativa consiste en indicar a qué nivel pertenece el dato en cuestión; siendo esta una decisión cualitativa, las salvaguardas a emplear son independientes del valor que el dato en sí tenga para la organización. La vía valorada asigna un nivel a las consecuencias que para la organización tendría el deterioro del dato. De esta forma se distingue entre las obligaciones legales y los perjuicios para el servicio, sin obviar ninguno de estos aspectos, ambos importantes.

Amenazas

5. Amenazas

Se presenta a continuación un catálogo de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: ▯ que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

5.1. [N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[N.1] Fuego	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema.	

[N.2] Daños por agua	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema.	

[N.*] Desastres naturales	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción:
otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ...

Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]).

Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.

5.2. [I] De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada.

[I.1] Fuego	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema.	

[I.2] Daños por agua	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	

[I.*] Desastres industriales	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.	

[I.3] Contaminación mecánica	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: vibraciones, polvo, suciedad, ...	

[I.4] Contaminación electromagnética	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información (electrónicos) ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ...	

[I.5] Avería de origen físico o lógico	
Tipos de activos: ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	

[I.6] Corte del suministro eléctrico	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información (electrónicos) ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: cese de la alimentación de potencia	

Descripción:
hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.

Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés *"Transient Electromagnetic Pulse Standard"*). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "*TEMPEST protection*", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara.

No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.

5.3. [E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas.

La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

[E.1] Errores de los usuarios	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc.	

[E.2] Errores del administrador	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción: equivocaciones de personas con responsabilidades de instalación y operación	

[E.3] Errores de monitorización *(log)*	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [T_S] trazabilidad del servicio 2. [T_D] trazabilidad de los datos
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...	

Salvaguardas

6. Salvaguardas

Las salvaguardas permiten hacer frente a las amenazas. Hay diferentes aspectos en los cuales puede actuar una salvaguarda para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo:

[PR] procedimientos, que siempre son necesarios; a veces bastan procedimientos, pero otras veces los procedimientos son un componente de una salvaguarda más compleja. Se requieren procedimientos tanto para la operación de las salvaguardas preventivas como para la gestión de incidencias y la recuperación tras las mismas. Los procedimientos deben cubrir aspectos tan diversos como van del desarrollo de sistemas la configuración del equipamiento.

[PER] política de personal, que es necesaria cuando se consideran sistemas atendidos por personal. La política de personal debe cubrir desde las fases de especificación del puesto de trabajo y selección, hasta la formación continua.

Soluciones técnicas, frecuentes en el entorno de las tecnologías de la información, que pueden ser

[SW] aplicaciones (software)

[HW] dispositivos físicos

[COM] protección de las comunicaciones

[FIS] seguridad física, de los locales y áreas de trabajo

La protección integral de un sistema de información requerirá una combinación de salvaguardas de los diferentes aspectos comentados, debiendo la solución final

1. estar equilibrada en los diferentes aspectos
2. tener en cuenta las salvaguardas adecuadas a cada tipo de activos
3. tener en cuenta las salvaguardas adecuadas a la dimensión de valor del activo
4. tener en cuenta las salvaguardas adecuadas a la amenaza a conjurar

Las salvaguardas, especialmente las técnicas, varían con el avance tecnológico

- porque aparecen tecnologías nuevas,
- porque van desapareciendo tecnologías antiguas,
- porque cambian los [tipos de] activos a considerar,
- porque evolucionan las posibilidades de los atacantes o
- porque evoluciona el catálogo de salvaguardas disponibles.

En consecuencia, este catálogo de salvaguardas no entra en la selección de paquetes o productos a instalar, limitándose a determinar requisitos que deberán ser satisfechos por la solución práctica que se elija.

6.1. Salvaguardas de tipo general

Son aquellas que se refieren al buen gobierno de la seguridad con efectos beneficiosos sobre todo tipo de activos.

- Organización de la seguridad: roles, comités, ...
- Política corporativa de seguridad de la información
- Gestión de privilegios: adjudicación, revisión y terminación
- Procedimientos de escalado y gestión de incidencias
- Procedimientos de continuidad de operaciones: emergencia y recuperación

- Auditoría, registro (certificación) y acreditación del sistema

6.2. Salvaguardas para la protección de los servicios

ciclo de vida	*protección del valor*
• Especificación del servicio • Desarrollo del servicio • Despliegue del servicio • Operación del servicio • Terminación del servicio	[A_S] → • Control de acceso [T_S] → • Registro de actuaciones • Registro de incidencias [D] → • Plan de continuidad

El control de acceso es un servicio de salvaguarda recurrente que se aplica en múltiples tipos de activos: acceso a los servicios, acceso a las aplicaciones, acceso al sistema operativo, acceso a los soportes de información, acceso físico a las instalaciones, etc. En todos ellos se requiere un sistema de identificación y autenticación que determine quién es el aspirante (sea persona u otro programa) y se coordine con el sistema de gestión de privilegios.

Los mecanismos de identificación y autenticación son múltiples y pueden combinarse de diferentes formas. Cabe destacar los siguientes:

- **contraseñas**: útil para sistemas que soportan poco riesgo, o como complemento a otros mecanismos
- **certificados digitales**: útil en sistemas expuestos a amenazas de repudio
- **dispositivos (tokens o tarjetas)**: útil en sistemas que soportan riesgo elevado o requisitos de urgente disponibilidad
- **características biométricas**: útil para identificar personas, que no roles.

6.3. Salvaguardas para la protección de los datos / información

organización	*protección del valor*
• Carácter personal, si procede • documento de seguridad • Clasificación, si procede • Gestión de claves, si se emplea cifrado	[A_D] → • Control de acceso • Firma electrónica [T_D] → • Registro de actuaciones • Registro de incidencias [D] → • Copias de respaldo [I] → • Detección y recuperación [C] → • Cifrado (preventivo) • Marcado (persecución)

[D] Datos / información

[D] Datos / Información	
código:	**nombre:**
descripción:	
propietario:	
responsable:	
tipo (marque todos los adjetivos que procedan):	
( ) [vr] datos vitales *(vital records)*	
( ) [com] datos de interés comercial	
( ) [adm] datos de interés para la administración pública	
( ) [int] datos de gestión interna	
( ) [source] código fuente	
( ) [exe] código ejecutable	
( ) [conf] datos de configuración	
( ) [log] registro de actividad *(log)*	
( ) [test] datos de prueba	
( ) [per] datos de carácter personal	
( ) [A] de nivel alto	
( ) [M] de nivel medio	
( ) [B] de nivel básico	
( ) [label] datos clasificados	
( ) [S] secreto	
( ) [R] reservado	
( ) [C] confidencial	
( ) [DL] difusión limitada	
( ) [SC] sin clasificar	

Valoración de los datos / información, típicamente en las siguientes dimensiones de seguridad:

[I] integridad

[C] confidencialidad

[A_D] autenticidad de quién accede a los datos

[T_D] trazabilidad de quién accede a los datos, cuándo y qué hace

Valoración		
dimensión	***valor***	***justificación***
[I]		
[C]		
[A_D]		
[T_D]		

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

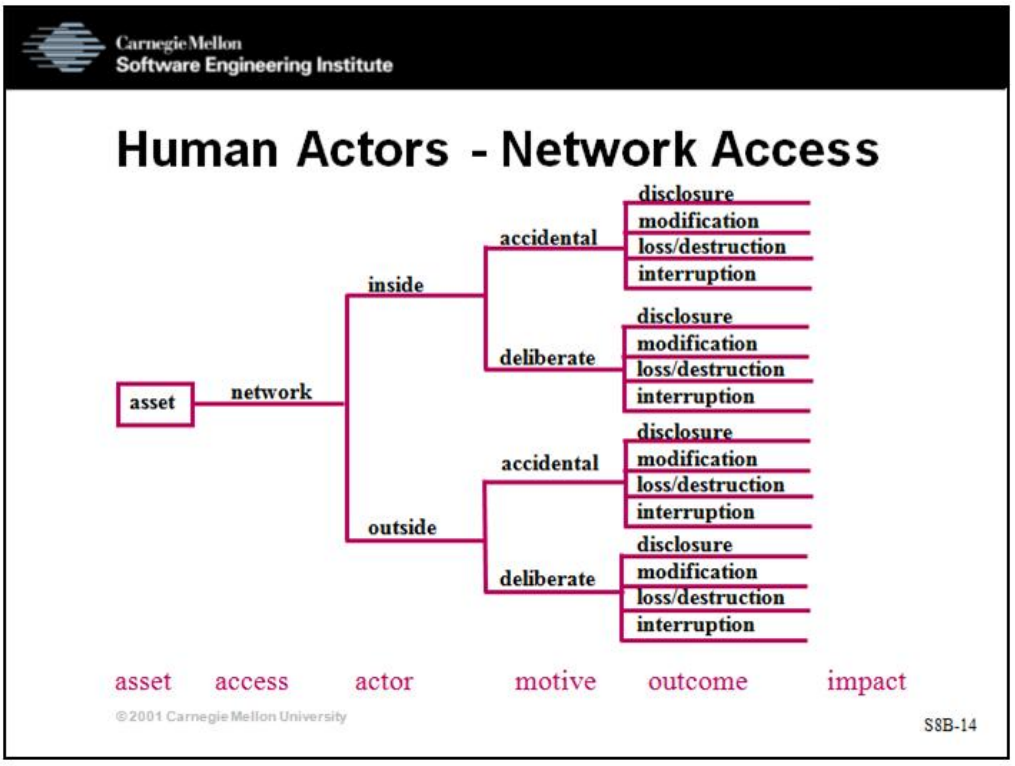
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

APÉNDICE F: METODOLOGIA OCTAVE

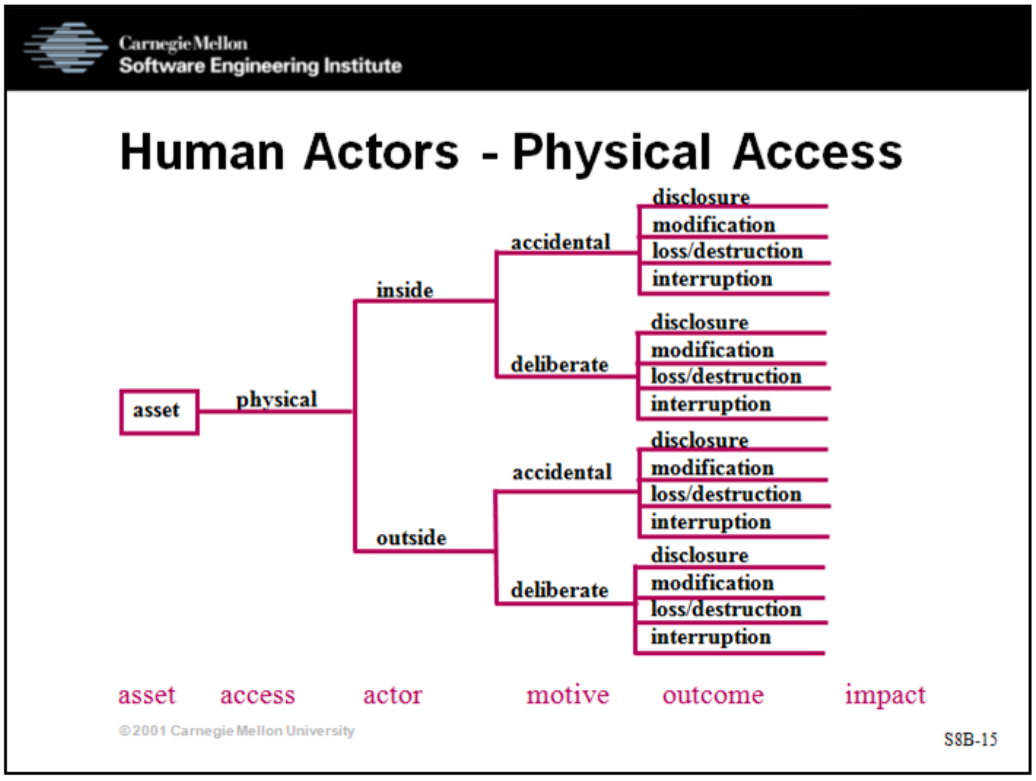
Árbol de riesgo basado en activos para actores humanos usando el acceso de red

OCTAVE Method Implementation Guide v2.0 Process 8 Workshop B Slides



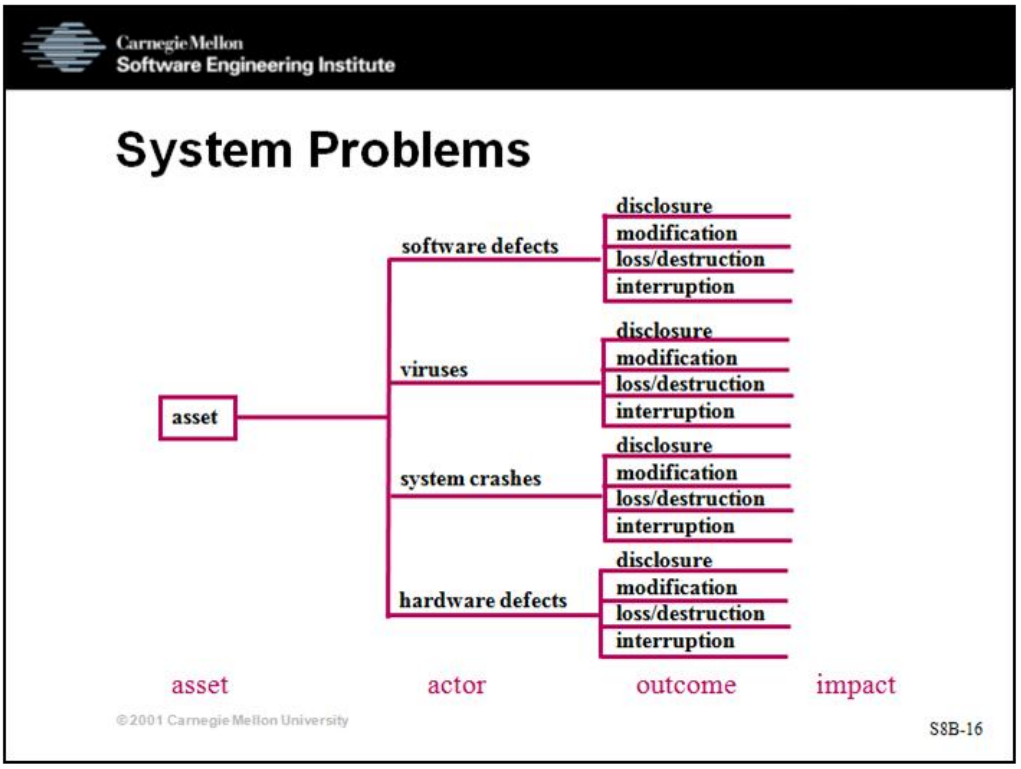
This viewgraph shows the asset-based risk tree for human actors using network access.

Árbol de riesgo basado en activos para actores humanos usando acceso físico



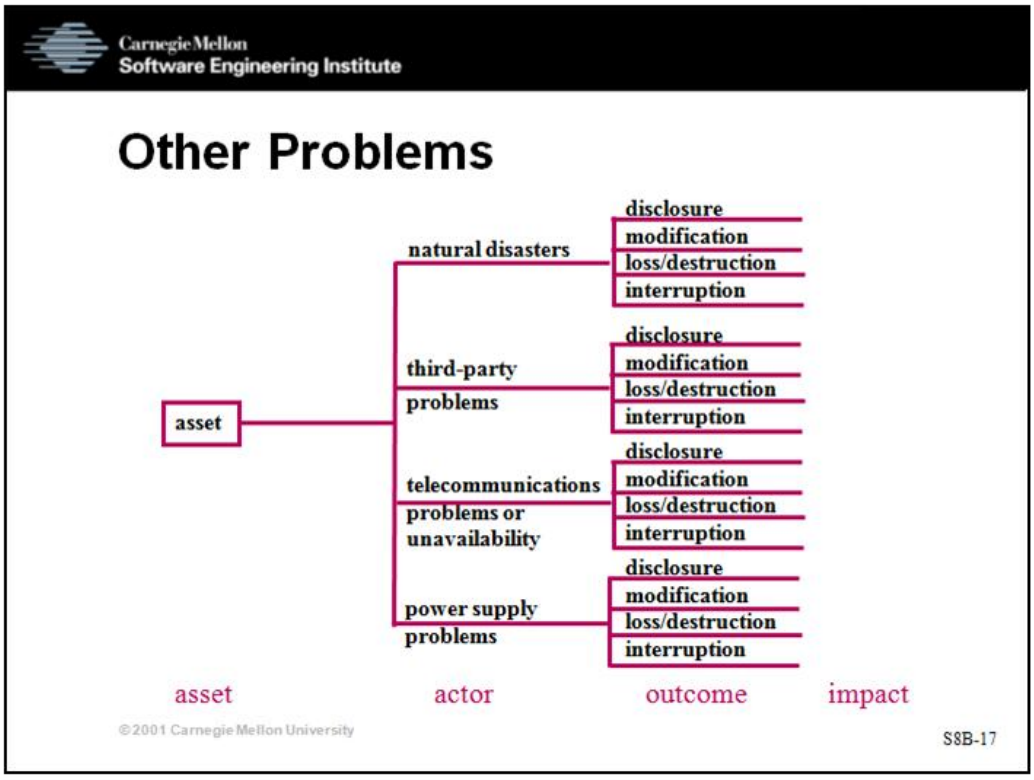
This viewgraph shows the asset-based risk tree for human actors using physical access.

Árbol de riesgo basado en activos para problemas de sistemas



This viewgraph shows the asset-based risk tree for system problems (for systems under your control).

Árbol de riesgo basado en activos para otros problemas



This viewgraph shows the asset-based risk tree for other problems (problems due to conditions out of your control).

Worksheet: Identificación de actives de información

Step 2

Information, Systems, and Applications	
System	**Information**
What systems do people in your organization need to perform their jobs?	*What information do people in your organization need to perform their jobs?*

	Information, Systems, and Applications
Applications and Services	**Other Assets**
What applications and services do people in your organization need to perform their jobs?	*What other assets are closely related to these assets?*

Gestión de vulnerabilidades

12. Vulnerability Management

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
There is a documented set of procedures for managing vulnerabilities, including • selecting vulnerability evaluation tools, checklists, and scripts • keeping up to date with known vulnerability types and attack methods • reviewing sources of information on vulnerability announcements, security alerts, and notices • identifying infrastructure components to be evaluated • scheduling of vulnerability evaluations • interpreting and responding to the evaluation results • maintaining secure storage and disposition of vulnerability data	Very Much	Somewhat	Not At All	Don't Know
Vulnerability management procedures are followed and are periodically reviewed and updated.	Very Much	Somewhat	Not At All	Don't Know
Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area: The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.	Very Much	Somewhat	Not At All	Don't Know

12. Vulnerability Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

Worksheet: activos críticos

Step 6	Step 7
Critical Asset	**Rationale for Selection**
What is the critical information?	*Why is this information critical to the organization?*

Step 9
Related Assets
Which assets are related to this information?
Systems: Applications:
Other:

Step 8

Description	
Who uses the information?	*Who is responsible for the information?*

Step 10		**Step 11**
Security Requirements		**Most Important Security Requirement**
What are the security requirements for this information? *(Hint: Focus on what the security requirements should be for this information, not what they currently are.)*		*Which security requirement is most important for this information?*
❑ Confidentiality	Only authorized personnel can view _____.	❑ Confidentiality ❑ Integrity ❑ Availability ❑ Other
❑ Integrity	Only authorized personnel can modify _____.	
❑ Availability	_____ must be available for personnel to perform their jobs. Unavailability cannot exceed _____ hour(s) per every _____ hours.	
❑ Other	_____ _____	

Perfiles básicos de riesgos

Human Actors Using Network Access — **Basic Risk Profile**

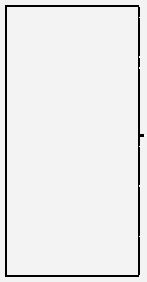
Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Asset — **Access** — **Actor** — **Motive** — **Outcome**



network

inside

outside

accidental

deliberate

disclosure

modification

loss, destruction

interruption

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
inside / accidental / disclosure						
inside / accidental / modification						
inside / accidental / loss, destruction						
inside / accidental / interruption						
inside / deliberate / disclosure						
inside / deliberate / modification						
inside / deliberate / loss, destruction						
inside / deliberate / interruption						
outside / accidental / disclosure						
outside / accidental / modification						
outside / accidental / loss, destruction						
outside / accidental / interruption						
outside / deliberate / disclosure						
outside / deliberate / modification						
outside / deliberate / loss, destruction						
outside / deliberate / interruption						

Basic Risk Profile

Human Actors Using Network Access

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence: Very | Somewhat | Not At All
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|
☐	|--------|--------|

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

Strategic						Operational								
1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy &	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys	9. Sys & Net	10. Monitor IT	11. Authen &	12. Vul Mgmt	13. Encryption	14. Sec Arch &	15. Incident
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	■	■	☐	☐	☐	☐	☐	☐	☐

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑

APÉNDICE G: ANEXO B NORMA ISO/IEC 27005:2008

Annex B
(informative)

Identification and valuation of assets and impact assessment

B.1 Examples of asset identification

To perform asset valuation, an organization first needs to identify its assets (at an appropriate level of detail). Two kinds of assets can be distinguished:

- The primary assets:
  - Business processes & activities
  - Information
- The supporting assets (on which the primary elements of the scope rely) of all types:
  - Hardware
  - Software
  - Network
  - Personnel
  - Site
  - Organization's structure

B.1.1 The identification of primary assets

To describe the scope more accurately, this activity consists in identifying the primary assets (business processes and activities, information). This identification is carried out by a mixed work group representative of the process (managers, information systems specialists and users).

The primary assets are usually the core processes and information of the activity in the scope. Other primary assets such as the organization's processes can also be considered, which will be more appropriate for drawing up an information security policy or a business continuity plan. Depending on the purpose, some studies will not require an exhaustive analysis of all the elements making up the scope. In such cases, the study boundaries can be limited to the key elements of the scope.

Primary assets are of two types:

1 - Business processes (or sub-processes) and activities, for example:

- Processes whose loss or degradation make it impossible to carry out the mission of the organization
- Processes that contain secret processes or processes involving proprietary technology
- Processes that, if modified, can greatly affect the accomplishment of the organization's mission
- Processes that are necessary for the organization to comply with contractual, legal or regulatory requirements

2 – Information:

More generally, primary information mainly comprises:

- Vital information for the exercise of the organization's mission or business
- Personal information, as can be defined specifically in the sense of the national laws regarding privacy
- Strategic information required for achieving objectives determined by the strategic orientations
- High-cost information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost

Processes and information that are not identified as sensitive after this activity will have no defined classification in the remainder of the study. This means that even if such processes or information are compromised, the organization will still accomplish the mission successfully.

However, they will often inherit controls implemented to protect the processes and information identified as sensitive.

B.1.2 List and description of supporting assets

The scope consists of assets that should be identified and described. These assets have vulnerabilities that are exploitable by threats aiming to impair the primary assets of the scope (processes and information). They are of various types:

Hardware

The hardware type consists of all the physical elements supporting processes.

Data processing equipment (active)

Automatic information processing equipment including the items required to operate independently.

Transportable equipment

Portable computer equipment.

Examples: laptop computer, Personal Digital Assistant (PDA).

Fixed equipment

Computer equipment used on the organization's premises.

Examples: server, microcomputer used as a workstation.

Processing peripherals

Equipment connected to a computer via a communication port (serial, parallel link, etc.) for entering, conveying or transmitting data.

Examples: printer, removable disc drive.

Data medium (passive)

These are media for storing data or functions.

Electronic medium

An information medium that can be connected to a computer or computer network for data storage. Despite their compact size, these media may contain a large amount of data. They can be used with standard computing equipment.

Examples: floppy disc, CD ROM, back-up cartridge, removable hard disc, memory key, tape.

Other media

Static, non-electronic media containing data.

Examples: paper, slide, transparency, documentation, fax.

Software

Software consists of all the programmes contributing to the operation of a data processing set.

Operating system

This includes all the programmes of a computer making up the operational base from which all the other programmes (services or applications) are run. It includes a kernel and basic functions or services. Depending on the architecture, an operating system may be monolithic or made up of a micro-kernel and a set of system services. The main elements of the operating system are all the equipment management services (CPU, memory, disc, and network interfaces), task or process management services and user rights management services.

Service, maintenance or administration software

Software characterised by the fact that it complements the operating system services and is not directly at the service of the users or applications (even though it is usually essential or even indispensable for the global operation of the information system).

Package software or standard software

Standard software or package software are complete products commercialised as such (rather than one-off or specific developments) with medium, release and maintenance. They provide services for users and applications, but are not personalised or specific in the way that business applications are.

Examples: data base management software, electronic messaging software, groupware, directory software, web server software, etc.

Business application

Standard business application

This is commercial software designed to give users direct access to the services and functions they require from their information system in their professional context. There is a very wide, theoretically limitless, range of fields.

Examples: accounts software, machine tool control software, customer care software, personnel competency management software, administrative software, etc.

Specific business application

This is software in which various aspects (primarily support, maintenance, upgrading, etc.) have been specifically developed to give users direct access to the services and functions they require from their information system. There is a very wide, theoretically unlimited, range of fields.

Examples: Invoice management of telecom operators' customers, real time monitoring application for rocket launching.

Network

The network type consists of all telecommunications devices used to interconnect several physically remote computers or elements of an information system.

Medium and supports

Communications and telecommunications media or equipment are characterised mainly by the physical and technical characteristics of the equipment (point-to-point, broadcast) and by the communication protocols (link or network - levels 2 and 3 of the OSI 7-layer model).

Examples: Public Switching Telephone Network (PSTN), Ethernet, GigabitEthernet, Asymmetric Digital Subscriber Line (ADSL), wireless protocol specifications (e.g. WiFi 802.11), Bluetooth, FireWire.

Passive or active relay

This sub-type includes all devices that are not the logical terminations of communications (IS vision) but are intermediate or relay devices. Relays are characterised by the supported network communication protocols. In addition to the basic relay, they often include routing and/or filtering functions and services, employing communication switches and routers with filters. They can often be administrated remotely and are usually capable of generating logs.

Examples: bridge, router, hub, switch, automatic exchange.

Communication interface

The communication interfaces of the processing units are connected to the processing units but are characterised by the media and supported protocols, by any installed filtering, log or warning generation functions and their capacities and by the possibility and requirement of remote administration.

Examples: General Packet Radio Service (GPRS), Ethernet adaptor.

Personnel

The personnel type consists of all the groups of people involved in the information system.

Decision maker

Decision makers are the owners of the primary assets (information and functions) and the managers of the organization or specific project.

Examples: top management, project leader.

Users

Users are the personnel who handle sensitive elements in the context of their activity and who have a special responsibility in this respect. They may have special access rights to the information system to carry out their everyday tasks.

Examples: human resources management, financial management, risk manager.

Operation/ Maintenance staff

These are the personnel in charge of operating and maintaining the information system. They have special access rights to the information system to carry out their everyday tasks.

Examples: system administrator, data administrator, back-up, Help Desk, application deployment operator, security officers.

Developers

Developers are in charge of developing the organization's applications. They have access to part of the information system with high-level rights but do not take any action on the production data.

Examples: business application developers.

Site

The site type comprises all the places containing the scope or part of the scope, and the physical means required for it to operate.

Location

External environment

This concerns all locations in which the organization's means of security cannot be applied.

Examples: homes of the personnel, premises of another organization, environment outside the site (urban area, hazard area)

Premises

This place is bounded by the organization's perimeter directly in contact with the outside. This may be a physical protective boundary obtained by creating physical barriers or means of surveillance around buildings.

Examples: establishment, buildings.

Zone

A zone is formed by a physical protective boundary forming partitions within the organization's premises. It is obtained by creating physical barriers around the organization's information processing infrastructures.

Examples: offices, reserved access zone, secure zone.

Essential services

All the services required for the organization's equipment to operate.

Communication

Telecommunications services and equipment provided by an operator.

Examples: telephone line, PABX, internal telephone networks.

Utilities

Services and means (sources and wiring) required for providing power to information technology equipment and peripherals.

Examples: low voltage power supply, inverter, electrical circuit head-end.

Water supply

Waste disposal

Services and means (equipment, control) for cooling and purifying the air.

Examples: chilled water pipes, air-conditioners.

Organization

The organization type describes the organizational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

Authorities

These are organizations from which the studied organization derives its authority. They may be legally affiliated or external. This imposes constraints on the studied organization in terms of regulations, decisions and actions.

Examples: administrating body, Head office of an organization.

Structure of the organization

This consists of the various branches of the organization, including its cross-functional activities, under the control of its management.

Examples: human resources management, IT management, purchasing management, business unit management, building safety service, fire service, audit management.

Project or system organization

This concerns the organization set up for a specific project or service.

Examples: new application development project, information system migration project.

Subcontractors / Suppliers / Manufacturers

These are organizations that provide the organization with a service or resources and bound to it by contract.

Examples: facilities management company, outsourcing company, consultancy companies.

B.2 Asset valuation

The next step after asset identification is to agree upon the scale to be used and the criteria for assigning a particular location on that scale to each asset, based on valuation. Because of the diversity of assets found within most organizations it is likely that some assets that have a known monetary value will be valued in the local unit of currency while others which have a more qualitative value may be assigned a value ranging, for example, from "very low" to "very high". The decision to use a quantitative scale versus a qualitative scale is really a matter of organizational preference, but should be relevant to the assets being valued. Both valuation types could be used for the same asset.

Typical terms used for the qualitative valuation of assets include words such as: negligible, very low, low, medium, high, very high, and critical. The choice and range of terms suitable to an organization is strongly dependent on an organization's needs for security, organizational size, and other organization specific factors.

Criteria

The criteria used as the basis for assigning a value to each asset should be written out in unambiguous terms. This is often one of the most difficult aspects of asset valuation since the values of some assets may have to be subjectively determined and since many different individuals are likely to be making the determination. Possible criteria used to determine an asset's value include its original cost, its replacement or re-creation cost or its value may be abstract, e.g. the value of an organization's reputation.

Another basis for the valuation of assets is the costs incurred due to the loss of confidentiality, integrity and availability as the result of an incident. Non-repudiation, accountability, authenticity and reliability should also be considered, as appropriate. Such a valuation would provide the important element dimensions to asset value, in addition to replacement cost, based on estimates of the adverse business consequences that would result from security incidents with an assumed set of circumstances. It is emphasized that this approach accounts for consequences that are necessary to factor into the risk assessment.

Many assets may during the course of valuation have several values assigned. For example: a business plan may be valued based on the labour expended to develop the plan, it might be valued on the labour to input the data, and it could be valued based on its value to a competitor. Each of the assigned values will most likely differ considerably. The assigned value may be the maximum of all possible values or may be the sum of some or all of the possible values. In the final analysis, which value or values are assigned to an asset should be carefully determined since the final value assigned enters into the determination of the resources to be expended for the protection of the asset.

Reduction to the common base

Ultimately, all asset valuations need to be reduced to a common base. This may be done with the aid of criteria such as those that follow. Criteria that may be used to assess the possible consequences resulting from a loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, or reliability of assets are:

- Violation of legislation and/or regulation
- Impairment of business performance
- Loss of goodwill/negative effect on reputation
- Breach associated with personal information
- Endangerment of personal safety
- Adverse effects on law enforcement
- Breach of confidentiality
- Breach of public order
- Financial loss
- Disruption to business activities
- Endangerment of environmental safety

Another approach to assess the consequences could be:

- Interruption of service
  - Inability to provide the service
- Loss of customer confidence
  - loss of credibility in the internal information system
  - damage to reputation
- Disruption of internal operation
  - disruption in the organization itself
  - additional internal cost
- Disruption of a third party's operation:
  - disruption in third parties transacting with the organization
  - various types of injury
- Infringement of laws / regulations:
  - inability to fulfill legal obligations
- Breach of contract:
  - inability to fulfill contractual obligations
- Danger to personnel / user safety:
  - danger for the organization's personnel and / or users
- Attack on users' private life
- Financial losses
- Financial costs for emergency or repair:
  - in terms of personnel,
  - in terms of equipment,
  - in terms of studies, experts' reports
- Loss of goods / funds / assets
- Loss of customers, loss of suppliers
- Judicial proceedings and penalties
- Loss of a competitive advantage
- Loss of technological / technical lead
- Loss of effectiveness / trust
- Loss of technical reputation
- Weakening of negotiating capacity

- Industrial crisis (strikes)
- Government crisis
- Dismissal
- Material damage

These criteria are examples of issues to be considered for asset valuation. For carrying out valuations, an organization needs to select criteria relevant to its type of business and security requirements. This might mean that some of the criteria listed above are not applicable, and that others might need to be added to the list.

Scale

After establishing the criteria to be considered, the organization should agree on a scale to be used organization-wide. The first step is to decide on the number of levels to be used. There are no rules with regard to the number of levels that are most appropriate. More levels provide a greater level of granularity but sometimes a too fine differentiation makes consistent assignments throughout the organization difficult. Normally, any number of levels between 3 (e.g. low, medium, and high) and 10 can be used as long as it is consistent with the approach the organization is using for the whole risk assessment process.

An organization may define its own limits for asset values, like "low", "medium", or "high". These limits should be assessed according to the criteria selected (e.g. for possible financial loss, they should be given in monetary values, but for considerations such as endangerment of personal safety, monetary valuation can be complex and may not be appropriate for all organizations). Finally, it is entirely up to the organization to decide what is considered as being "low" or a "high" consequence. A consequence that might be disastrous for a small organization could be low or even negligible for a very large organization.

Dependencies

The more relevant and numerous the business processes supported by an asset, the greater the value of this asset. Dependencies of assets on business processes and other assets should be identified as well since this might influence the values of the assets. For example, the confidentiality of data should be kept throughout its life-cycle, at all stages, including storage and processing, i.e. the security needs of data storage and processing programmes should be directly related to the value representing the confidentiality of the data stored and processed. Also, if a business process is relying on the integrity of certain data being produced by a programme, the input data of this programme should be of appropriate reliability. Moreover, the integrity of information will be dependent on the hardware and software used for its storage and processing. Also, the hardware will be dependent on the power supply and possibly air conditioning. Thus information about dependencies will assist in the identification of threats and particularly vulnerabilities. Additionally, it will help to assure that the true value of the assets (through the dependency relationships) is given to the assets, thereby indicating the appropriate level of protection.

The values of assets on which other assets are dependent may be modified in the following way:

- If the values of the dependent assets (e.g. data) are lower or equal to the value of the asset considered (e.g. software), its value remains the same

- If the values of the dependent asset (e.g. data) is greater, then the value of the asset considered (e.g. software) should be increased according to:

    - The degree of dependency
    - The values of the other assets

An organization may have some assets that are available more than once, like copies of software programmes or the same type of computer used in most of the offices. It is important to consider this fact when doing the asset valuation. On one hand, these assets are overlooked easily, therefore care should be taken to identify all of them; on the other hand, they could be used to reduce availability problems.

Output

The final output of this step is a list of assets and their values relative to disclosure (preservation of confidentiality), modification (preservation of integrity, authenticity, non-repudiation and accountability), non-availability and destruction (preservation of availability and reliability), and replacement cost.

B.3 Impact assessment

An information security incident can impact more than one asset or only a part of an asset. Impact is related to the degree of success of the incident. As a consequence, there is an important difference between the asset value and the impact resulting from the incident. Impact is considered as having either an immediate (operational) effect or a future (business) effect that includes financial and market consequences.

Immediate (operational) impact is either direct or indirect.

Direct:

a) The financial replacement value of lost (part of) asset

b) The cost of acquisition, configuration and installation of the new asset or back-up

c) The cost of suspended operations due to the incident until the service provided by the asset(s) is restored

d) Impact results in a information security breach

Indirect:

a) Opportunity cost (financial resources needed to replace or repair an asset would have been used elsewhere)

b) The cost of interrupted operations

c) Potential misuse of information obtained through a security breach

d) Violation of statutory or regulatory obligations

e) Violation of ethical codes of conduct

As such, the first assessment (with no controls of any kind) will estimate an impact as very close to the (combination of the) concerned asset value(s). For any next iteration for this (these) asset(s), the impact will be different (normally much lower) due to the presence and the effectiveness of the implemented controls.

APÉNDICE H : ANEXO C NORMA ISO/IEC 27005:2008

Annex C
(informative)

Examples of typical threats

The following table gives examples of typical threats. The list can be used during the threat assessment process. Threats may be deliberate, accidental or environmental (natural) and may result, for example, in damage or loss of essential services. The following list indicates for each threat type where D (deliberate), A (accidental), E (environmental) is relevant. D is used for all deliberate actions aimed at information assets, A is used for all human actions that can accidentally damage information assets, and E is used for all incidents that are not based on human actions. The groups of threats are not in priority order.

Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Disturbance due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulses	A, D, E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	D
	Theft of equipment	D
	Retrieval of recycled or discarded media	D
	Disclosure	A, D
	Data from untrustworthy sources	A, D
	Tampering with hardware	D
	Tampering with software	A, D
	Position detection	D

Type	Threats	Origin
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A, D
	Software malfunction	A
	Breach of information system maintainability	A, D
Unauthorised actions	Unauthorised use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Forging of rights	D
	Denial of actions	D
	Breach of personnel availability	A, D, E

Particular attention should be paid to human threat sources. These are specifically itemized in the following table:

Origin of threat	Motivation	Possible consequences
Hacker, cracker	Challenge Ego Rebellion Status Money	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g. cyber stalking) • Fraudulent act (e.g. replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge Political Gain Media Coverage	• Bomb/Terrorism • Information warfare • System attack (e.g. distributed denial of service) • System penetration • System tampering

Origin of threat	Motivation	Possible consequences
Industrial espionage (intelligence, companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Defence advantage • Political advantage • Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g. virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

APÉNDICE I: ANEXO D NORMA ISO/IEC 27005:2008

Annex D
(informative)

Vulnerabilities and methods for vulnerability assessment

D.1 Examples of vulnerabilities

The following table gives examples for vulnerabilities in various security areas, including examples of threats that might exploit these vulnerabilities. The lists can provide help during the assessment of threats and vulnerabilities, to determine relevant incident scenarios. It is emphasized that in some cases other threats may exploit these vulnerabilities as well.

Types	Examples of vulnerabilities	Examples of threats
Hardware	Insufficient maintenance/faulty installation of storage media	Breach of information system maintainability
	Lack of periodic replacement schemes	Destruction of equipment or media
	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing
	Sensitivity to electromagnetic radiation	Electromagnetic radiation
	Lack of efficient configuration change control	Error in use
	Susceptibility to voltage variations	Loss of power supply
	Susceptibility to temperature variations	Meteorological phenomenon
	Unprotected storage	Theft of media or documents
	Lack of care at disposal	Theft of media or documents
	Uncontrolled copying	Theft of media or documents
Software	No or insufficient software testing	Abuse of rights
	Well-known flaws in the software	Abuse of rights
	No 'logout' when leaving the workstation	Abuse of rights
	Disposal or reuse of storage media without proper erasure	Abuse of rights
	Lack of audit trail	Abuse of rights
	Wrong allocation of access rights	Abuse of rights
	Widely-distributed software	Corruption of data
	Applying application programs to the wrong data in terms of time	Corruption of data
	Complicated user interface	Error in use
	Lack of documentation	Error in use
	Incorrect parameter set up	Error in use
	Incorrect dates	Error in use

	Lack of identification and authentication mechanisms like user authentication	Forging of rights
	Unprotected password tables	Forging of rights
	Poor password management	Forging of rights
	Unnecessary services enabled	Illegal processing of data
	Immature or new software	Software malfunction
	Unclear or incomplete specifications for developers	Software malfunction
	Lack of effective change control	Software malfunction
	Uncontrolled downloading and use of software	Tampering with software
	Lack of back-up copies	Tampering with software
	Lack of physical protection of the building, doors and windows	Theft of media or documents
	Failure to produce management reports	Unauthorised use of equipment
Network	Lack of proof of sending or receiving a message	Denial of actions
	Unprotected communication lines	Eavesdropping
	Unprotected sensitive traffic	Eavesdropping
	Poor joint cabling	Failure of telecommunication equipment
	Single point of failure	Failure of telecommunication equipment
	Lack of identification and authentication of sender and receiver	Forging of rights
	Insecure network architecture	Remote spying
	Transfer of passwords in clear	Remote spying
	Inadequate network management (resilience of routing)	Saturation of the information system
	Unprotected public network connections	Unauthorised use of equipment
Personnel	Absence of personnel	Breach of personnel availability
	Inadequate recruitment procedures	Destruction of equipment or media
	Insufficient security training	Error in use
	Incorrect use of software and hardware	Error in use
	Lack of security awareness	Error in use
	Lack of monitoring mechanisms	Illegal processing of data
	Unsupervised work by outside or cleaning staff	Theft of media or documents
	Lack of policies for the correct use of telecommunications media and messaging	Unauthorised use of equipment

Site	Inadequate or careless use of physical access control to buildings and rooms	Destruction of equipment or media
	Location in an area susceptible to flood	Flood
	Unstable power grid	Loss of power supply
	Lack of physical protection of the building, doors and windows	Theft of equipment
Organization	Lack of formal procedure for user registration and de-registration	Abuse of rights
	Lack of formal process for access right review (supervision)	Abuse of rights
	Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties	Abuse of rights
	Lack of procedure of monitoring of information processing facilities	Abuse of rights
	Lack of regular audits (supervision)	Abuse of rights
	Lack of procedures of risk identification and assessment	Abuse of rights
	Lack of fault reports recorded in administrator and operator logs	Abuse of rights
	Inadequate service maintenance response	Breach of information system maintainability
	Lack or insufficient Service Level Agreement	Breach of information system maintainability
	Lack of change control procedure	Breach of information system maintainability
	Lack of formal procedure for ISMS documentation control	Corruption of data
	Lack of formal procedure for ISMS record supervision	Corruption of data
	Lack of formal process for authorization of public available information	Data from untrustworthy sources
	Lack of proper allocation of information security responsibilities	Denial of actions
	Lack of continuity plans	Equipment failure
	Lack of e-mail usage policy	Error in use
	Lack of procedures for introducing software into operational systems	Error in use
	Lack of records in administrator and operator logs	Error in use
	Lack of procedures for classified information handling	Error in use
	Lack of information security responsibilities in job descriptions	Error in use

APÉNDICE J: FORMATOS DE LA METODOLOGIA PROPUESTA MARISGSI

1. Formato usado para la identificación de los activos críticos:

ACT_ID: Identificación de activos

Activo	Descripción	Codificación	Ubicación	Propietario
Activos (1… N)	Breve descripción del activo	Código	Donde se encuentra	Persona, proceso, entidad, etc.

2. Formato usado para la documentación de los activos críticos e identificar el nivel de impacto que tiene cada uno.

ACT_DOC: Documentación de activos

Activo	Descripción	Clasificación del activo (alto, medio, bajo impacto a la institución)
Activo 1 …….. Activo N	Breve descripción	Indicar que nivel de impacto tiene

3. Valores referenciales de frecuencia y degradación, que permiten visualizar el nivel de impacto:

REFERENCIA DE FRECUENCIA Y DEGRADACIÓN

DEGRADACION (Daño causado)	*ALTO*	Impacto moderado	Impacto alto	Impacto alto	Impacto alto
	MEDIO	Impacto bajo	Impacto moderado	Impacto alto	Impacto alto
	BAJO	Impacto bajo	Bajo impacto	Impacto moderado	Impacto alto
NIVEL DE IMPACTO		Poco frecuente	Normal	Frecuente	Muy frecuente
		VALOR DE FRECUENCIA			

4. Formato usado para identificar las amenazas y las vulnerabilidades y su nivel de exposición sobre el activo:

VUL_ID: IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

ACTIVOS	AMENAZAS (¿Qué es lo que preocupa?)	VULNERABILIDADES (¿Cómo puede ocurrir?)	NIVEL DE EXPOSICIÓN (A, M, B)
Activo 1			
Activo 2			
……			
Activo n			

Leyenda: A = Alto, M = Medio, B = Bajo

5. Formato usado para determinar el impacto total generado sobre una entidad:

EST_IMP: DETERMINACIÓN DEL IMPACTO

ACTIVO / FACTOR	FACTOR 1	FACTOR 2	…….……	FACTOR N	IMPACTO A LA ENTIDAD	IMPACTO
Activo 1						
Activo 2						
Activo …						
Activo N						
				IMPACTO TOTAL		

Donde:

- **Activo:** Nombre del activo
- **Impacto a la entidad:** este valor es tomado del cuadro 13: documentación de los activos, nivel de exposición (Alto, Medio, Bajo), usando la siguiente escala numérica para representar el impacto: Alto = 10, Medio = 5, Bajo = 2.
- **Impacto:** resultado total de la suma de los factores multiplicado por el valor del impacto a la entidad.

6. Formato para la valoración de los factores que inciden en la determinación del impacto de un activo:

VAL_FAC: Valoración de factores

Nº FACTOR	FACTOR	VALORACIÓN (Alto, Medio, Bajo)
1	**Factor 1**	
2	**Factor 2**	
n	**Factor n**	

7. Formato que se obtiene al finalizar el proceso de análisis de riesgos a una entidad o parte de ella:

ANÁLISIS DE RIESGOS

ACTIVOS	AMENAZAS ¿Qué es lo que preocupa?	VULNERABILIDAD ¿Cómo puede ocurrir?	NIVEL DE EXPOSICIÓN (A,M,B)	DESCRIPCIÓN DE CONTROLES ACTUALES	DESCRIPCIÓN DE CONTROLES NUEVOS
Activo 1					
Activo 2					
…….					
Activo n					

EJEMPLOS:

VUL_ID: Identificación de amenazas y vulnerabilidades

ACTIVOS	AMENAZAS (¿Qué es lo que preocupa?)	VULNERABILIDADES (¿Cómo puede ocurrir?)	NIVEL DE EXPOSICIÓN (A, M, B)
Contratos de docentes	Robo	Falta del sistema de protección de documentación	A
Red de datos	Acceso no autorizado	Falta de mecanismos de seguridad informáticos	M
Red de datos	Error de operación	Falla de los procedimientos de seguridad del SGSI	A
Red de datos	Fallo del sistema	Falta del procedimiento de seguridad. Falta de backup de repuesto	A

ACT_ID: Identificación de activos

Activo	Descripción	Codificación	Ubicación	Propietario
Contratos de docentes	Documentos de contratos de cada uno de los docentes de la institución	COD0001	Recursos humanos	Gte. Recursos humanos
Red de datos	Sistema que maneja los datos personales de cada estudiante de la institución	RDA0001	Dpto. de control de estudios	Jefe de control de estudios

ACT_DOC: Documentación de activos

Activo	Descripción	Clasificación del activo (alto, medio, bajo impacto a la institución)
Contratos de docentes	Documentos de contratos de cada uno de los docentes de la institución	A
Red de datos	Sistema que maneja los datos personales de cada estudiante de la institución	A

VAL_FAC: Valoración de factores

Nº FACTOR	FACTOR	VALORACIÓN (Alto=10, Medio=5, Bajo=2)
1	Licencias de Windows Server	**5**
2	Mantenimiento de software	**5**
3	Costo de hardware	**10**
4	Mantenimiento de hardware	**2**

EST_IMP: Determinación del impacto

ACTIVO / FACTOR	FACTOR 1	FACTOR 2	FACTOR 3	FACTOR 4	IMPACTO A LA ENTIDAD	IMPACTO
Contratos de docentes		5		2	10	70
Red de datos	5	5	10	2	10	220
				IMPACTO TOTAL		290

Donde:

- **Activo:** Nombre del activo
- **Impacto a la entidad:** este valor es tomado del cuadro 13: documentación de los activos, nivel de exposición (Alto, Medio, Bajo), usando la siguiente escala numérica para representar el impacto: Alto = 10, Medio = 5, Bajo = 2.
- **Impacto:** resultado total de la suma de los factores multiplicado por el valor del impacto a la entidad.

ANÁLISIS DE RIESGOS

ACTIVOS	AMENAZAS (¿Qué es lo que preocupa?)	VULNERABILIDADES (¿Cómo puede ocurrir?)	NIVEL DE EXPOSICIÓN (A, M, B)	DESCRIPCIÓN DE CONTROLES EXISTENTES	DESCRIPCIÓN DE CONTROLES NUEVOS
Contratos de docentes	Robo	Falta del sistema de protección de documentación	A	Protección por contraseña	Mejorar nivel de contraseña
Red de datos	Acceso no autorizado	Falta de mecanismos de seguridad informáticos	M	Ninguno	Definir control de acceso
Red de datos	Error de operación	Falla de los procedimientos de seguridad del SGSI	A	Ninguna política de backup	Establecer rutinas para hacer backup