UNIVERSIDAD DE CARABOBO
FACULTAD DE CIENCIAS ECONÓMICAS Y SOCIALES
DIRECCIÓN DE POSTGRADO
SECCIÓN DE GRADO

POST GRADO FACES
ESTUDIOS SUPERIORES PARA GRADUADOS
Facultad de Ciencias Económicas y Sociales
Universidad de Carabobo

ACTA DE DISCUSIÓN DE TRABAJO DE GRADO

En atención a lo dispuesto en los Artículos 127, 128, 137, 138 y 139 del Reglamento de Estudios de Postgrado de la Universidad de Carabobo, quienes suscribimos como Jurado designado por el Consejo de Postgrado de la Facultad de Ciencias Económicas y Sociales, de acuerdo a lo previsto en el Artículo 135 del citado Reglamento, para estudiar el Trabajo de Especialización titulado:

"SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN COMO MECANISMO PARA LA ACTUALIZACIÓN DE LAS MEDIDAS DE PROTECCIÓN DE DEPARTAMENTO DE INFORMÁTICA DE UNA UNIVERSIDAD PÚBLICA"

Presentado para optar al grado de ESPECIALISTA EN GERENCIA DE PROTECCION INDUSTRIAL por el(la) aspirante:

GOMEZ L., JOSE R.
C.I.: 9.277.997

Realizado bajo la tutoría de el(la) Prof. RIVAS L., ARIANA T., titular de la cédula de identidad Nº. 14.230.118

Habiendo examinado el Trabajo presentado, se decide que el mismo está Aprobado

En Bárbula, a los 14 dias del mes de octubre de 2015

Prof. Gasparini C., Victor G. (PRESIDENTE)
C.I.: 4561580
Fecha: 14/10/2015

Prof. Hamidian F., Benito F.
C.I.: 06318306
Fecha: 14/10/2015

UNIVERSIDAD DE CARABOBO Facultad de Ciencias Económicas y Sociales POST GRADO FACES SECCION DE GRADO AREA ADMINISTRATIVA

Prof. Sequera O., Jose L.
C.I.: 12101023
Fecha: 14/10/2015

UNIVERSIDAD DE CARABOBO
FACULTAD DE CIENCIAS ECONÓMICAS Y SOCIALES
ESTUDIOS DE POSTGRADO
ESPECIALIZACIÓN EN PROTECCIÓN INDUSTRIAL
CAMPUS BÁRBULA

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN COMO MECANISMO PARA LA ACTUALIZACIÓNDE LAS MEDIDAS DE PROTECCIÓN DELDEPARTAMENTO DE INFORMÁTICA DE UNA UNIVERSIDAD PÚBLICA

Autor:

Ing. Gómez José

Bárbula, Octubre de 2015

UNIVERSIDAD DE CARABOBO
FACULTAD DE CIENCIAS ECONÓMICAS Y SOCIALES
ESPECIALIZACIÓN EN PROTECCIÓN INDUSTRIAL
CAMPUS BÁRBULA

CONSTANCIA DE ACEPTACIÓN

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN COMO MEDIO PARA LA ACTUALIZACIÓN DE LAS MEDIDAS DE PROTECCIÓN DEL DEPARTAMENTO DE INFORMÁTICA DE UNA UNIVERSIDAD PÚBLICA

Tutora:
Esp. Ariana Rivas

Aceptado en la Universidad de Carabobo
Facultad de Ciencias Económicas y Sociales
Área de Estudios de Postgrado
Maestría en Administración del Trabajo y Relaciones Laborales
Por: Ariana Rivas
C.I. 14.230.118

Bárbula, Febrero de 2015

2

Universidad de Carabobo.
Facultad de Ciencias Económicas y Sociales
Dirección de Estudios de Postgrado.
Especiación en Gerencia de Protección Industrial

POST GRADO FACES
ESTUDIOS SUPERIORES PARA GRADUADOS
Facultad de Ciencias Económicas y Sociales
Universidad de Carabobo

VEREDICTO

Nosotros, Miembros del Jurado designado para la evaluación del Trabajo de Grado titulado: ***"SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN COMO MECANISMO PARA LA ACTUALIZACIÓN DE LAS MEDIDAS DE PROTECCIÓN DEL DEPARTAMENTO DE INFORMÁTICA DE UNA UNIVERSIDAD PÚBLICA".*** Presentado por el (la) ciudadano (a): *Gómez L. José R.* Titular de la Cédula de identidad **Nº V.** *9.277.997.* Para optar al título de **Especialización en Gerencia de Protección Industrial**, el mismo reúne los requisitos para ser considerado como:

Aprobado

Nombre, Apellido	C.I.	Firma del Jurado
Victor Carpanini	11761580	
Jose L. Segovia	V-12101023	
Benito Hamidian	06318306	

Bárbula, Octubre 2015

UNIVERSIDAD DE CARABOBO
FACULTAD DE CIENCIAS ECONÓMICAS Y SOCIALES
ESTUDIOS DE POSTGRADO
ESPECIALIZACIÓN EN PROTECCIÓN INDUSTRIAL
CAMPUS BÁRBULA

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN COMO MECANISMO PARA LA ACTUALIZACIÓN DE LAS MEDIDAS DE PROTECCIÓN DELDEPARTAMENTO DE INFORMÁTICA DE UNA UNIVERSIDAD PÚBLICA

Autor: Gómez, José

Tutora: Rivas,Ariana

Fecha: Octubre, 2015

RESUMEN

El presente trabajo especial de Grado, tuvo como objetivo principal determinar la seguridad de los sistemas de información como mecanismo para la actualización de las medidas de protección en el departamento de informática de una universidad pública. Para esto fue necesario, analizar los riesgos presentes en los sistemas de información, conocer la seguridad de dichos sistemas con base en los riesgos, debilidades y fortalezas encontradas en el Departamento sujeto a estudio, para luego formular algunas estrategias de seguridad a considerar con base en los resultados obtenidos a partir de la valoración realizada. Para lograr tales objetivos se trabajó mediante una metodología de campo, basada en un diseño no experimental donde se recolecto la información mediante la aplicación del cuestionario de seguridad, a la muestra que estuvo conformada por tres (3) administradores de Sistemas del Departamento sujeto a estudio, el cual sirvió como base para realizar el análisis de riesgo basado en el Método Mosler. Los resultados del análisis indican que existe vulnerabilidad en los riesgo: Incendio y Sabotaje Informático y fuga de información, por lo cual se sugiere como estrategias crear un plan de Prevención y Emergencia, que se refuerce con medidas de capacitación al personal y formación de brigada de emergencia y tomar medidas de refuerzo en cuanto a los aspectos organizativos, técnicos y legales de manera de que se sigua un proceso controlado y las tareas se realicen de la forma más segura posible.

Descriptores: Seguridad**,** Protección,Sistemas de Información, Riesgos, Método Mosler

ÍNDICE GENERAL

ÍNDICE DE CUADROS

INTRODUCCIÓN

La seguridad en cualquier organización debe afrontar hoy en día el creciente desafío que significa dirigir esfuerzos de prevención y protección hacia los activos humanos, materiales e intangibles que les han sido encomendado custodiar. Su reto principal será actuar sobre la cultura, generando confianza, alineando la estructura hacia los objetivos organizacionales y transformando la estrategia en resultados, a través de las personas. Para lograr esto, tal como lo plantea Grimald & Simonds(1996), será necesario pprofundizaren el conocimiento de la misión, visión y los valores de la organización, para poder desarrollar políticas de seguridad que coadyuven al cumplimiento de los objetivos y afiancen una cultura de seguridad corporativa.

La Gestión del Riesgo busca lograr conocimiento, lo más realista posible, de aquellas circunstancias que podrían afectar a los procesos o servicios, causando daños o pérdidas, de modo que puedan establecerse prioridades y asignarse requisitos de seguridad para afrontar convenientemente dichas situaciones. Tal como señala Mañas (2011) estos riesgos que pueden ser de muy diversa naturaleza, cobran especial importancia cuando afectan el ámbito de las tecnologías de la información, debido a su imbricación en gran cantidad de los servicios que regulan en la sociedad actual.

Es por lo antes mencionado, que se presenta a continuación un trabajo especial de grado en el que se tiene como objetivo principal determinar la seguridad de los sistemas de información como mecanismo para la

actualización de las medidas de protección en el departamento de informática de una universidad pública.

Para ello, fue necesario analizar los riesgos presentes en los sistemas de información del Departamento de Informática sujeto a estudio, así como conocer la seguridad de los sistemas de información con base en los riesgos, debilidades y fortalezas encontradas para posteriormente, formular algunas estrategias de seguridad a considerar con base en los resultados obtenidos a partir de la valoración realizada.

Para efectos de esta investigación, se procedió a organizar el contenido en 4 capítulos, para una mejor compresión del estudio.

Capítulo I, se plantea la problemática de la situación actual, se presenta el Objetivo General, así como, los objetivos específicos donde se establecen los procedimientos para su realización. Asimismo se presenta la importancia y la justificación del estudio.

Capítulo II, se hace mención los antecedentes de la investigación, donde se consideran algunos trabajos de diferentes autores, las bases teóricas que sustentan la investigación, así como el basamento legal de la misma.

Capítulo III, conformado por el Marco Metodológico, se definió el procedimiento para lograr el desarrollo del estudio, la investigación, diseño, alcance, las técnicas y los instrumentos aplicados en la recolección de los datos.

Capítulo IV: El desarrollo de los resultados y la presentación de los mismos. Finalmente se detallan las conclusiones y recomendaciones pertinentes, así como, las referencias empleadas.

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

Un hecho mundial que viene dándose a nivel de las industrias y organizaciones, es que en la medida en que el crecimiento económico así como el empresarial se ha desarrollado, la manera en la que se almacena, resguarda o se protege la información también lo ha hecho. Los sistemas informáticos han sido la gran herramienta que ha permitido tanto a pequeñas como grandes empresas hacer el resguardo de uno de los principales bienes con el que esta puede contar: la información. Estos sistemas que son el eje del funcionamiento y control del mundo empresarial han sido adsorbidos de igual forma por organizaciones e instituciones educativas, políticas, sociales, judiciales entre otras, que tras los avances que ofrece la informática ven necesario la implementación de estos sistemas a fin de marchar al mismo paso.

En tal sentido, de acuerdo con Soler (2009:8) un sistema de información "es aquel que transforma datos de entrada, los procesa, los almacena para su posterior uso y distribuye la información a los usuarios internos y externos de la organización", esto implica que por medio de su empleo se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas.

Aunado a esto, los sistemas de información de acuerdo con Martínez (2010:35) se entienden como “un recurso vital para toda organización, y el buen manejo de estos puede significar la diferencia entre el éxito o el fracaso para todos los proyectos que se emprendan dentro de un organismo que busca el crecimiento y el éxito”. En general los sistemas de información, representa el bien intangible de mayor valor con el que cualquier organización o empresa puede contar.

No obstante, pese a las grandes ventajas que representan los sistemas de información, las amenazas y la vulnerabilidad de estos es una realidad; es por ello que surge en esta investigación la necesidad de evaluar la seguridad de los sistemas de información y con ello los riesgos a los que se expone la información así como su resguardo y seguridad, es un tema que cobra cada día mayor interés. Dicho interés de acuerdo con Cedeño (2008:52) se debe a que “los sistemas de información concentran los datos en archivos de computadoras que son una vía de fácil acceso”, esto hace posible que un gran número de usuarios, personas o grupos externos a la organización no autorizados, los manipule, tal situación conlleva a que la información sea mucho más asequible, y susceptible a modificaciones que puedan producir destrucción, fraude o error.

Dentro de ese marco, otro punto que cobra valor es cuando los sistemas de información fallan o no funcionan como es debido, las compañías que dependen mucho de ellos no pueden funcionar de la forma en la que lo hacen habitualmente y cuanto más tiempo permanezcan inactivos, más graves serán las consecuencias para la organización. De allí que sea necesario establecer las medidas de seguridad adecuadas, las cuales deben atender a las necesidades de seguridad de la información de la empresa, permitiendo implementar y operar controles con los que se pueda manejar los riesgos, a toda vez que se pueda monitorear y revisar el

desempeño del sistema de seguridad que se desee implementar, así como su actualización y mejora continua, de manera de minimizar conflictos y contar con planes de resguardo de la información realmente confiables.

En este orden de ideas, aun cuando los riesgos a los que se exponen los sistemas de información son asociados frecuentemente al ataque con virus, software malignos, entre otros; debe tenerse en cuenta que el riesgo al que la información se expone va más allá de aspectos programables, la estructura que los resguarda es también vital, lo que hace necesario exponer y estudiar los riesgos de los sistemas de seguridad de una manera amplia.

En este punto, tal como lo indica Sánchez (2009:40) “la seguridad es uno de los aspectos más olvidados a la hora del diseño de un sistema informático”. Por consiguiente, si se toma en cuenta este último punto, puede aseverarse que el riesgo a los que se exponen los sistemas de información represente un punto de gran relevancia para aquellas instituciones u organizaciones en donde tales sistemas comprende el centro de sus funciones, por lo que resulta trascendente considerar, conocer y evaluar a fondo este tipo de riesgos; un ejemplo claro de un organismos donde los sistemas de información son más que simples datos, son las instituciones educativas, tal como lo expresa Barcos (2008)

> la información y la tecnología utilizada para apoyar su adquisición, procesamiento, almacenamiento, recuperación y difusión han adquirido importancia estratégica en todo tipo de organizaciones y también en las educativas de todos los niveles del sistema, sean públicas o privadas y tanto si planifican, coordinan evalúan como si ejecutan acciones educativas en forma directa, dejando de ser elementos que sólo tenían que ver con apoyo operativo y administrativo o que servían para cumplir con lo estipulado en un reglamento, norma o programa.(p. 210)

Esto se debe a que las organizaciones educativas son productoras y usuarias de la información al mismo tiempo, son responsables de la existencia de canales horizontales de circulación de la información y de la incorporación de información del contexto. Como señala Barcos (2008:226) “los sistemas de información están incluidos en todos los modelos de evaluación de la calidad y son tomados en cuenta como predictores para el alcance de los resultados”; esto hace que los mismos constituyan una importante e imprescindible dimensión de los procesos de la educación y administración universitaria.

Un ejemplo de lo antes expuesto se aprecia en una investigación llevada a cabo por Barcos (2008), en la cual resalta la relevancia de los sistemas de información para universidades, en esta destaca que “los sistemas son esenciales para la gestión, para lograr enriquecer los resultados de la adopción de decisión y también para informar las acciones de las universidades a la sociedad”. También hace algunas reflexiones respecto de los sistemas de informaciones en los procesos de evaluación y acreditación y muestra los defectos detectados en universidades europeas y Latinoamericanas. Asimismo, se plantean requerimientos y funciones de este importante recurso y un especial énfasis en desarrollarlos adecuadamente para optimizar el funcionamiento y para impulsar la integración entre instituciones educativas en el contexto global.

Siguiendo este mismo enfoque, la Universidad Tecnológica Nacional de Buenos Aires, Argentina; se ha incorporado en la tarea de implementar sus propias políticas de seguridad de la información, basándosele las características establecidas en el Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional publicado por la Oficina Nacional de Tecnología de Información (ONTI) de Argentina.

Así mismo, con el propósito de que dicha implementación pueda realizarse en forma ordenada y gradual, la universidad encomendó a su comité de seguridad de la información, la tarea de elaborar y coordinar la ejecución de un plan de acción para el año 2009que fijara objetivos vinculados a los temas de seguridad.

En este orden de ideas en Venezuela se evidencian mejoras en este aspecto, tal este caso de la Universidad Lisandro Alvarado del Estado Lara, Venezuela; implemento un Sistema de Gestión de la Seguridad Centro de Tecnología de Información y Comunicación (CTIC) del Decanato de Ciencias y Tecnología de acuerdo al estándar internacional ISO/IEC 27001:2005, esto con el fin de adaptar una adopción de una metodología sólida para la gestión del riesgo que permitiera descubrir los puntos vulnerables del sistema de información que tomar los correctivos necesarios para su tratamiento.

Bajo esta perspectiva, un caso cuya competencia se hace de interés es el Departamento de Informática de la Universidad pública sujeta a estudio, el cual es la unidad organizativa que realiza funciones de naturaleza técnica y de servicios en materia de administración, producción y desarrollo de sistemas de información, con la finalidad de satisfacer las necesidades de las dependencias de la Institución. Este departamento, cuyo norte está centrado en el orden y la evolución del sistema de información de la universidad, comprende un eje cuyo resguardo y seguridad deben ser vistos con verdadera importancia.

En relación a este último punto, es evidente como pese a contar con tecnología de avanzada para el resguardo de la información que manejan, no ha sido evaluada la seguridad de los sistemas. Asimismo en el departamento carecen de análisis de riesgos y evaluación de la seguridad por ningún medio o herramienta certificado. Esto representa desde el punto de vista de

la seguridad de los sistemas de información vulnerabilidad, pues al no evaluar el sistema deja abierta la posibilidad de cualquier tipo de falla.

Cabe señalar, que en la actualidad debido a los constantes acontecimientos sociales la casa de estudio sujeta a estudio ha sido de manera reiterada foco de alteraciones de orden público; estas necesariamente deben ser vistas como amenazas para esta institución y en especial para el Departamento de Informática, quien cuenta con todas sus bases de datos en estas instalaciones.

En tal sentido, las consecuencias que pueden surgir al hacer caso omiso a la protección de los sistemas de seguridad son entre otras: perdida de información, sabotaje, robo y usurpación de identidad, filtración de información confidencial, daño de proyectos, pérdida de horas de trabajo por las reparaciones así como por la reconfiguración de los equipos y redes, indisponibilidad de aplicaciones y servicios. Es por esto que es importante considerar que el análisis periódico para los diferentes procesos del departamento de Informática, puede ayudar a identificar riesgos antes que éstos se materialicen y por lo que estas entidades serán menos propensas a sufrir incidentes que pudieron ser evitados.

Consecuentemente, tal como lo señala Ibarra (2008:59) cualquiera que sea el tamaño, finalidad, complejidad del negocio o de la plataforma tecnológica, ninguna organización debe desconocer los riesgos que se plantean para cada uno de los procesos que constituyen su actividad y, una vez identificados, no debe dejar de gestionarlos. Si esto último ocurriera, irremediablemente se afectaría su desempeño pudiendo, inclusive, verse obligada a cesar su actividad.

Sin embargo, gracias a los avances en el área de seguridad, en la actualidad existen herramientas como la gestión de riesgos, que permiten

atender y prevenir aquellas situaciones que pueden causar un daño real sobre la información desde el aspecto físico y que brindan una adecuada protección.

Si bien estos instrumentos no son tan sencillos como incorporar un equipo o una pieza de software, son herramientas cuya aplicabilidad y esfuerzo vale la pena; una efectiva gestión del riesgo, necesariamente deberán conocerse las situaciones que pueden afectar a la organización, es decir de qué debe protegerse, cuál es su información y sus recursos críticos, y si las medidas que ha implementado para preservarlos evitarán o minimizarán cualquier impacto negativo.

De este modo y sobre las bases de las ideas expuestas, se plantean las siguientes interrogantes: ¿Qué tipo de riesgos se encuentran presentes en los sistemas de información del departamento de informática de la universidad sujeta a estudio? ¿Qué valor puede dársele a la seguridad de los sistemas de información con base en los riesgos, debilidades y fortalezas encontradas? ¿Cuáles son las estrategias de seguridad a considerar con base en los resultados obtenidos a partir de la valoración realizada? Por medio de estas interrogantes se pretende desarrollar de una manera clara y precisa los aspectos de la seguridad de la institución objeto de estudio, permitiendo con esto aportar estadísticas, actualizar información y brindar recomendaciones.

Objetivos de la Investigación

Objetivo general

Determinar la seguridad de los sistemas de información como mecanismo para la actualización de las medidas de protección en el departamento de informática de una universidad pública.

Objetivos Específicos

- Analizar los riesgos presentes en los sistemas de información del Departamento de Informática de una universidad pública.
- Conocer la seguridad de los sistemas de información con base en los riesgos, debilidades y fortalezas encontradas.
- Formular algunas estrategias de seguridad a considerar con base en los resultados obtenidos a partir de la valoración realizada.

Justificación de la Investigación

En el campo de la seguridad de la información, el problema de las vulnerabilidades ha dado lugar a un nuevo escenario. Ya no resultan suficientes las soluciones simples o aisladas sino que se hace necesario implementar seguridad en profundidad, que proteja todos los activos de acuerdo con su criticidad, y también contemple la capacitación y la concientización a los empleados sobre las nuevas amenazas. La presente investigación busca brindar un aporte en primer lugar, social, pues a partir de dicho estudio se podrá conocer los riesgos, debilidades y fortalezas del sistema de información, lo cual beneficiará no sólo a la casa de estudio sino a sus empleados, estudiantes y comunidad, pues se podrán tomar acciones que fortalezcan y otorguen una mayor seguridad en cuanto a los servicios que esta ofrece, pudiendo satisfacer de un mejor modo todas las necesidades de las dependencias de la Institución.

Aunado a ello, se indagaran los elementos necesarios conducentes a la protección de los recursos de información de la universidad y la tecnología utilizada para su procesamiento, frente a amenazas externas, deliberadas o

accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asimismo al desarrollar este estudio se realizan planteamientos actualizados del cómo y de qué manera debe darse la seguridad física de los sistemas de información rompiendo así los viejos paradigmas de la seguridad simple, permitiendo exponer a nivel teórico la complejidad de la misma pero dejando en claro la sencillez de su estructura cuando es enfocada y trabajada en concomitancia con las necesidades de cada sistema, siguiendo directrices y procedimientos diseñado para esto.

Por otra parte, este trabajo especial de grado tiene una aplicabilidad en el contexto académico en el desarrollo de su fundamentación teórica, puesto que, este estudio podría llenar algunos vacíos de conocimientos acerca de la importancia que tiene, para las organizaciones e instituciones educativas en general, la búsqueda de alternativas que permitan ofrecer soluciones a las problemáticas presentes en los procesos de desarrollo, producción, soporte y administración de los sistemas de información.

Finalmente, esta investigación se adscribe a la línea de investigación: Educación y Trabajo de LOINET, por cuanto el propósito de la investigación está en concordancia con las características que asume el sistema ocupacional, la formación y la dinámica de las transformaciones en el mundo del trabajo, ofreciendo con esto un aporte a la cultura en seguridad, a la universidad, a la comunidad, a sus trabajadores y empleados y aquellos estudiantes en formación.

CAPÍTULO II

MARCO TEÓRICO

El desarrollo del marco teórico tiene gran importancia en las investigaciones, pues con él, el investigador pretende sustentar teóricamente el estudio, valiéndose de anteriores investigaciones y de puntos de vista de otros autores, en cuyo análisis se pueda encontrar apoyo significativo para la interpretación de los resultados. La metodología de este marco estará conformada por los antecedentes de la investigación, los fundamentos teóricos y la definición de términos básicos.

Antecedentes de la Investigación

Los antecedentes de la investigación, según Abreu (200:92) “se refieren a los estudios previos relacionados con el problema planteado, es decir, investigaciones realizadas anteriormente y que guardan alguna vinculación con el objetivo de estudio”. En este sentido, se han ubicado estudios y otros documentos que ofrecen una orientación y la posibilidad de ahondar en cada tema, con lo cual se pretende obtener información de interés para el desarrollo de la investigación en curso.

Montesino (2013) en su trabajo de grado titulado: Gestión automatizada e integrada de controles de seguridad informática. En esta investigación presentada ante la Universidad de las Ciencias Informáticas (UCI), La Habana, cuba; se propone un modelo para la gestión automatizada e integrada de controles de seguridad informática, basado en sistemas de gestión de información y eventos de seguridad (SIEM), que posibilita aumentar la efectividad de los controles implementados y disminuir la complejidad de la gestión de la seguridad de la información.

Se define el concepto de automatización en el contexto de la seguridad informática y se determinan los controles que pueden ser automatizados. Como parte de la investigación se seleccionan un grupo de indicadores que permiten medir de forma automatizada la efectividad de los controles, se propone además una guía para la aplicación del modelo propuesto y se describe una posible implementación del mismo utilizando el sistema SIEM de software libre Open Source Security Information Management (OSSIM).

En tal sentido, el estudio indica que los responsables de la gestión de la seguridad informática en las instituciones podrán aumentar la efectividad de los controles y disminuir la complejidad del proceso de gestión mediante la aplicación del modelo propuesto. El trabajo pudiera resultar útil también para los desarrolladores de sistemas SIEM en el sentido de aumentar las funcionalidades de estos sistemas y aumentar su potencial de automatización.

El aporte de esta investigación al trabajo en curso, se encuentra principalmente en la evidencia de que la gestión de la seguridad informática es un proceso complejo que implica el establecimiento de un gran número de controles en un entorno dinámico de múltiples amenazas. Resaltando el hecho de que para reducir la complejidad y aumentar la efectividad de la gestión de la seguridad de la información es posible automatizar determinadas acciones y controles. La automatización de controles de seguridad informática implica que la operación, monitorización y la revisión de los mismos se realice de forma automática por herramientas de hardware y software, sin intervención humana en esas acciones.

Ruiz (2010) su trabajo de grado titulado: Un modelo para el desarrollo de sistemas de detección de situaciones de riesgo capaces de integrar información de fuentes heterogéneas. Aplicaciones. Esta investigación se presentó ante la Universidad de Granada España, optar al título de Magister

en Ciencia de Datos e Ingeniería de Computadores, tuvo como finalidad proponer un modelo base para el desarrollo de sistemas de seguridad inteligentes, que se caractericen por ser flexibles ante la inclusión de otras fuentes de información sobre el entorno, escalables para introducir nuevas funcionalidades y portables a cualquier escenario de estudio. Como ejemplo de aplicaciones del modelo propuesto, se presentan tres sistemas inteligentes para la detección de las siguientes situaciones de alerta: la presencia de riesgo de atropello, la identificación de peligro por niños en zonas de tráfico y la detección de intrusiones.

Esta investigación muestra como los sistemas de vigilancia han sido, y son, ampliamente usados para mantener la seguridad en entornos monitorizados. Sin embargo, la vigilancia tradicional, que consiste en publicar, mediante monitores, el vídeo que recogen las cámaras de vigilancia, implica la atención constante de un operador humano para que no pase desapercibido cualquier peligro existente.

Por lo cual ha sido necesario que surjan nuevos sistemas de seguridad inteligentes para paliar la carga del vigilante y evitar la presencia de riesgos no identificados por la falta de atención o la presencia de fatiga en el operador. Estos sistemas tienen como objetivo analizar e interpretar de forma automática la escena y llamar la atención del personal únicamente en los momentos que sea necesario, con el fin de avisarles de ciertos riesgos o peligros en tiempo real.

Por otra parte, este trabajo hace mención de los grandes avances en la vigilancia inteligente, recalcando que aún existen muchos aspectos a mejorar en los sistemas de seguridad. Muchos de ellos se han diseñado para ser aplicados en entornos muy concretos y cumplir un fin específico, lo que repercute en que no puedan ser aplicados en otros espacios y que su escalabilidad sea baja. No obstante, en esta investigación se hace mención

al hecho de unificar todas las tecnologías de seguridad, y se llevar a cabo un proceso de integración de la información obtenida, puede lograrse un sistema de vigilancia mucho más potente que disponga de todos los datos unificados en la etapa de toma de decisiones.

De Freitas (2009), en su trabajo titulado: Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Para optar al título de Especialista en Telecomunicaciones. Este trabajo presentado ante la Universidad Simón Bolívar, Caracas, Venezuela; propone conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información que están en custodia en la Dirección de Servicios Telemáticos (DST) de la Universidad Simón Bolívar 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 permitió recoger información detallada usando una variedad de sistemas de recolección de datos, como entrevistas semi-estructuradas, 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 las Normas ISO-27001:2007. Se concluye que cada uno de los elementos en custodia de la DST es de suma importancia para la Universidad Simón Bolívar, por lo que se sugiere la aplicación de algunos controles establecidos en las normas ISO, para cada uno de dichos activos.

Esta investigación resalta como aporte que para escogencia de los controles de seguridad se estos deben justificarse con base a las conclusiones obtenidas del análisis, evaluación y tratamiento del riesgo a los cuales se someten los activos de información. Asimismo, se destaca que

pese a que existen muchos métodos para el cálculo de riesgos de activos de información, se debe escoger el que más se adapte a las características de la empresa.

Fundamentos teóricos

Sistemas de Información

En la actualidad los sistemas de información constituyen el objeto de estudio para numerosos autores y sus definiciones son planteadas desde diferentes enfoques, parte de estos enunciados son los siguientes:

Según Andreu, Ricart y Valor (1991), se entiende por sistema de información:

> Conjunto integrado de procesos, principalmente formales, desarrollados en un entorno usuario-computador, que operando sobre un conjunto de datos estructurados de una organización, recopilan, procesan y distribuyen selectivamente la información necesaria para la operatividad habitual de la organización y las actividades propias de la dirección de la misma. (p.89)

Por otra parte, de acuerdo con Peña (2006: 54) un sistema de información es un “conjunto de elementos interrelacionados con el propósito de prestar atención a las demandas de información de una organización, para elevar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones”, esto quiere decir que los sistemas de información son un conjunto que comprende herramientas que permiten el manejo de la información a fin de ser el soporte de las disposiciones tomadas por las organizaciones.

Otros autores como Peralta (2008:67), define sistema de información como “conjunto de elementos que interactúan entre sí con el fin de apoyar

las actividades de una empresa (…) teniendo muy en cuenta el equipo computacional necesario para que el sistema de información pueda operar y el recurso humano que interactúa con el Sistema de Información (…)" En tal sentido, un sistema de información según este autor es la unificación de factores entre las actividades y los requerimientos de la organización vinculados con la información que genera la misma.

Atendiendo a los elementos planteados, en la presente investigación se consideran sistemas de información, al conjunto de elementos encargados de administrar y optimizar el uso de los recursos informáticos, custodiar la información y mantener una estructura de datos cónsona con las demandas de los usuarios, así como una red de datos con calidad de enlace, garantizando la operatividad y condiciones de seguridad en el acceso al portal, intranet y sistemas de información desarrollados en la Dirección de Informática de la Universidad de Carabobo (DIUC).

En este mismo orden de ideas, para Payren, (2004:81) los elementos que se requieren para el funcionamiento del sistema de información son: "el componente físico (computadoras y sus complementos), programas (manejo de datos), el recurso humano (alimentación de datos y utilización de los resultados), datos e información".

De igual forma, señala Payren (2004:68) que un sistema de información desarrolla cuatro actividades básicas: "entrada, almacenamiento, procesamiento de datos y salida de información".

La actividad de entrada de información que se define como un proceso en el cual se toman los datos requeridos para procesar la información; las entradas se pueden hacer manual o automáticamente. En la primera el usuario aporta la información directamente y en la segunda, los datos provienen de otros sistemas.

Por su parte el almacenamiento de la información es un proceso en el cual se guarda la información en archivos que pueden ser recuperados en cualquier momento. En cuanto al procesamiento de la información, este permite la transformación de los datos fuentes en resultados por la aplicación de mecanismos o indicadores que soporten la toma decisiones. Finalmente la salida de información la cual representa la capacidad de un sistema para sacar la información procesada hacia otro sistema o usuario.

Fundamentos de la Seguridad Informática

La seguridad de los sistemas de información es un punto que afecta a todos los aspectos de una organización. Conseguir la seguridad adecuada requiere del conocimiento y domino de los fundamentos que la conforman. En primer lugar se encuentra la fiabilidad, la cual definida es definida por Mifsud (2012:53) como: la probabilidad de que un sistema se comporte tal y como se espera de él. En general, un sistema será seguro o fiable si se pueden garantizar tres aspectos: Confidencialidad: acceso a la información solo mediante autorización y de forma controlada. Integridad: modificación de la información solo mediante autorización. Disponibilidad: la información del sistema debe permanecer accesible mediante autorización.

Seguidamente se encuentra confidencialidad la cual es definida por Mifsud (2012:53) como: el acceso a la información solo mediante autorización y de forma controlada. En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

Siguiendo este orden, se tiene la integridad la cual de acuerdo con Mifsud (2012:53) está relacionada con la modificación de la información solo

mediante autorización. En general, el término 'integridad' hace referencia a una cualidad de 'íntegro' e indica "Que no carece de ninguna de sus partes." y relativo a personas "Recta, proba, intachable." En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado. El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información. La integridad hace referencia a: la integridad de los datos (el volumen de la información) y la integridad del origen (la fuente de los datos, llamada autenticación). A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos.

Por último se describe la disponibilidad la cual para Mifsud (2012:54) es quien representa la información del sistema en cuanto a la accesibilidad de la misma mediante autorización. En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos. En términos de seguridad informática “un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados”. Es decir, un sistema es disponible si permite no estar disponible.

En síntesis, las bases de la seguridad informática consisten en mantener el equilibrio adecuado entre estos cuatro factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.

Seguridad de los sistemas de información

Debido a la creciente dependencia de las organizaciones hacia la tecnología informática, se hace cada vez más imprescindible la necesidad de disponer de controles, de auditorías, normas y estándares de trabajo que garanticen la calidad y seguridad de los sistemas de información. Según Bran (2010), la seguridad de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial.

Por su parte Huerta, (2008:2) señala que la seguridad consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial".

Asimismo la norma ISO/IEC 27001 (*Information technology - Security techniques - Information security management systems - Requirements*) aprobada y publicada en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC), hace mención a la seguridad física indicando lo siguiente:

> La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Esto se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. En un sentido amplio referente a la presente

investigación se entiende como todos aquellos mecanismos - generalmente de prevención y detección - destinados a proteger físicamente cualquier recurso del sistema.

Siendo la seguridad física un aspecto de gran importancia pero que con frecuencia resulta olvidado; en muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema. Esto motiva que en determinadas situaciones un atacante se decline por aprovechar vulnerabilidades físicas en lugar de lógicas, ya que posiblemente le sea más fácil robar una cinta con una imagen completa del sistema que intentar acceder a él mediante fallos en el software.

Amenazas físicas y su tipología

Según Mifsud (2012) las amenazas físicas se pueden agrupar de acuerdo al medio o raíz que las produzca tal como se muestra a continuación:

En primer lugar se encuentra el acceso físico, en el cual de acuerdo con el autor, debe tenerse en cuenta que cuando existe acceso físico a un recurso ya no existe seguridad sobre él. Supone entonces un gran riesgo y probablemente con un impacto muy alto. A menudo se descuida este tipo de seguridad. El ejemplo típico de este tipo es el de una organización que dispone de tomas de red que no están controladas, son libres.

Por otra parte, se encuentran las radiaciones electromagnéticas, las cuales provienen de cualquier aparato eléctrico emite radiaciones y que dichas radiaciones se puede capturar y reproducir, si se dispone del

equipamiento adecuado. Por ejemplo, un posible atacante podría 'escuchar' los datos que circulan por el cable telefónico. Es un problema que hoy día con las redes wifi desprotegidas, por ejemplo, vuelve a estar vigente.

En este mismo orden de ideas, se encuentran los desastres naturales los cuales son fenómenos naturales que si se produjeran tendrían un gran impacto y no solo en términos de sistemas informáticos, sino en general para la sociedad. Siempre hay que tener en cuenta las características de cada zona en particular. Las posibilidades de que ocurra una inundación no son las mismas en todas las regiones. Hay que conocer bien el entorno en el que están físicamente los sistemas informáticos.

Como último punto, se encuentran los desastres del entorno, dentro de este grupo estarían incluidos sucesos que, sin llegar a ser desastres naturales, pueden tener un impacto igual de importante si no se disponen de las medidas de salvaguardas listas y operativas. Puede ocurrir un incendio o un apagón y no tener bien definidas las medidas a tomar en estas situaciones o simplemente no tener operativo el SAI que debería responder de forma inmediata al corte de suministro eléctrico.

Gestión de la Seguridad de los Sistemas de Información

La gestión de riesgos de los sistema de información en adelante, SI, constituye la principal forma de hacer frente al problema de la seguridad de la información en las organizaciones, esta pasa a ser una labor de vital importancia ya no a nivel funcional si no ha nivel corporativo. De ella se desprende la planificación de la seguridad de los SI, y por ende las políticas y medidas de seguridad a implantar como también los objetivos, estrategias, y organización de la seguridad. La gestión de riesgos en los SI es una acción permanente cíclica y recurrente, es decir, se ha de realizar continuamente debido a los cambios del sistema y de su entorno.

Según Pérez y Campanero (2010:122) “la gestión de la seguridad involucra a tres ámbitos de la institución: la organización, el entorno físico y el entorno lógico o software de las telecomunicaciones”; estos pueden concebirse de acuerdo con estos autores de la siguiente forma:

La Organización, se considera el primer ámbito ya que un Plan de Seguridad limitado a los sistemas de información y procedente de los servicios de informática no garantizará la seguridad. La informática, al constituirse en sistema de información de la institución, formará parte de su infraestructura y penetran en sus funciones, modificando las formas de trabajar y las relaciones, constituyéndose en una parte de alto riesgo dentro de dicha institución. Por ello, la Dirección General debe desempeñar un papel de motor y de animación en materia de seguridad, aplicando el plan estratégico de seguridad, que dé lugar a reglamentos de régimen interior en materia de seguridad, plan de contingencia y plan de seguridad informática.

Todo esto requerirá, por supuesto, la implicación de todo el personal, debiendo dedicar una especial atención a la información, a la formación y a los ejercicios tácticos. Las responsabilidades deberán estar claramente definidas, así como la coordinación entre los responsables. Así, debería existir un servicio o sección de seguridad vinculado a una dirección general independiente. También deberá disponer de una responsable especialista en seguridad general y otro de seguridad informática, éste último ligado también al servicio de informática.

El segundo ámbito se relaciona con el entorno físico, ya que es necesario conocer el entorno circundante del edificio para así poder prevenir los riesgos de seguridad. Así, no es lo mismo un pequeño edificio rodeado de bosques, que uno situado sobre acantilados, ya que está claro que será más accesible a efectos delictivos el primero que el segundo.

De igual forma, no tendrá las mismas necesidades de sistemas de seguridad un edificio situado en zona de aluvión, o con posibles inundaciones, que un edificio situado en medio de una llanura castellana, o en zonas de tormentas seísmos, humedad, viento. Se deben implantar controles de acceso, sistemas antiparásitos en las redes eléctricas, sistemas de detección de incendios, sistemas de vigilancia y observación.

El tercero y último de los ámbitos es el entorno lógico, el cual según el equipo a proteger requerirá unas medidas de seguridad u otras. Está claro que si el equipo es un ordenador personal dedicado a escribir cartas o citas a pacientes, no requerirá las mismas medidas de seguridad que los que alberguen las historias clínicas de los pacientes.

Es decir, todo dependerá de lo crítico de la información y de su sensibilidad a ser utilizada de forma delictiva. Lo ideal es que los grandes ordenadores estén aislados lo más posible de las personas y del entorno, debiendo dedicarles salas cerradas y exclusivas para ellos. Los materiales que sean altamente ignífugos deberían separarse del ordenador, y se debería dotar a estas salas de sistemas anti-incendios, sistemas de aire acondicionado y detectores de humedad.

También será necesario asegurar la continuidad de servicio, por lo que será necesario dotar al ordenador de sistemas de alimentación ininterrumpida. En cuanto al material magnético de almacenamiento y copias de seguridad se deberán almacenar en armarios anti-incendios y en salas separadas del ordenador.

Etapas de la Gestión de riesgos

Según Bringas (2011:110), las etapas de la Gestión de riesgos comprende los siguientes aspectos:

Primera etapa o Identificación de Riesgos; es la primera etapa a emprender, para abordarla, hay que listar los recursos con los que cuente la organización, en segundo lugar se deben identificar las amenazas que constituyen riesgos para la organización, después de determinar las amenazas es necesario estimar qué tan factible es que suceda cada una de ellas.

Segunda etapa o Análisis de Riesgos, en esta se debe determinar la probabilidad de ocurrencia del riesgo y evaluar el impacto que tendría en el negocio en el caso de pasar a un siniestro. Tal determinación depende del conocimiento que se tenga del fenómeno en particular.

Tercera etapa o Priorización de Riesgos, esta etapa se lleva a cabo una vez concluida la de análisis de riesgos y tiene como objetivo determinar donde se centrará el esfuerzo en nuestro plan de gestión, en función de nuestros recursos y los objetivos de nuestro negocio

Cuarta etapa o Resolución del Riesgo, en esta se decide cómo hacer frente al riesgo, se debe adoptar un camino, con la evaluación del costo que puede tener para seguirlo. Entre las resoluciones que se puede estar: Evitar que el riesgo exista, trasladar el Riesgo (por ej.: pasarlo de un proceso critico a uno que no lo sea), asumir el riesgo (Aquí se establecen planes de contingencia), comunicar el riesgo, recordar el riesgo y eliminar el Riesgo

Quinta etapa o Planificación del Control de Riesgos, tiene como objetivo la planificación es obtener una serie de medidas (ya sean políticas, planes de contingencia, reglas etc.) para limitar los riesgos que atentan contra los SI (disminuir su probabilidad de ocurrencia).

Sexta etapa o Monitoreo de Riesgos, esta etapa debe estar en continua ejecución y servirá como medio para evaluar los efectos de los mecanismos

de seguridad implantados, permitirá ir mejorando el plan de control de riesgos como también permitirá que se reevalúen las probabilidades de ocurrencia de ciertos riesgos, existiendo la posibilidad que algunos desaparezcan o también que surjan nuevos riesgos que obligarán a la empresa a modificar su plan para hacerles frente.

Medidas de protección de la seguridad física de los sistemas de información

Según Misfud (2012) en general estas medidas se pueden agrupar en protección electrónica, incendios, condiciones climatológicas e instalaciones eléctricas a las cuales el autor se refiere de la siguiente manera:

La Protección electrónica, tiene como objetivo la detección de robos, intrusiones, asaltos e incendios mediante la utilización de sensores conectados a centrales de alarmas. Una central de alarma dispone de elementos de señalización encargados de comunicar al personal que hay una situación de emergencia. Si un elemento sensor instalado detecta una situación de riesgo, transmite inmediatamente el aviso a la central. La central procesa la información recibida y como respuesta emite señales sonoras o luminosas que alertan de la situación.

Los Incendios, en este aspectos el autor señala que los sistemas contra incendios normalmente no son muy buenos y provocan prácticamente el mismo daño que el propio fuego, sobre todo a los componentes electrónicos. Una solución podría ser la utilización de dióxido de carbono (alternativa del agua), pero es peligroso por su toxicidad para los propios empleados si quedan atrapados en el CPD.

Las condiciones climatológicas, en este aspecto la tecnología disponible, tanto a nivel de dispositivos como de software, es posible predecir

con mucha exactitud las condiciones climatológicas. Normalmente se reciben los avisos de tormentas, tempestades, huracanes, tifones y terremotos. En concreto, en el caso de los terremotos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detecten o tan intensos que provoquen la destrucción de edificios e incluso pérdida de vidas humanas.

La Instalación eléctrica, destaca pues para su funcionamiento los ordenadores necesitan electricidad y ésta es una de las principales áreas a tener en cuenta en la seguridad física.

De manera general, para que la seguridad de la información sea efectiva se requiere un enfoque global, en la medida en la que debe cubrir todas las áreas informacionales, e integradora, buscando la sinergia en la implantación de las medidas de seguridad. De poco puede servir la implantación de un potente software antivirus en el servidor de imágenes si no aseguramos su alimentación eléctrica mediante un SAI (Sistema de Alimentación Ininterrumpida) en caso de corte del suministro eléctrico.

En tal sentido, señala Martínez (2006:109) la seguridad de la información “debe comenzar con un análisis de riesgos para que la organización conozca las amenazas a las que está expuesta y decida qué nivel de riesgo está dispuesta a asumir”. Es elemental que si no se conocen los riesgos no será fácil decidir qué hacer. Es por ello que a partir de este análisis de riesgo deben tomarse las decisiones oportunas encaminadas a la implantación de las salvaguardas que permitan controlar y mitigar dichos riesgos.

En el proceso de decisión, la organización puede priorizar la implantación de las medidas de seguridad sobre la base de criterios económicos, temporales, etc. Mediante el análisis y gestión de los riesgos se consigue un enfoque global e integrado de la seguridad del sistema de

información. No obstante, debido a la diversidad y variabilidad de las amenazas a los que están expuestos los sistemas de información, ningún sistema de seguridad elimina completamente la posibilidad de verse afectado por una amenaza al sistema, más es posible lograr un sistema con niveles de seguridad altamente confiables.

Método Mosler

La Gestión del Riesgo se apoya en el Análisis de Riesgos conforme al proceso que permite identificar, estudiar y evaluar a través de las diferentes variables implicadas, los potenciales eventos que afecten los objetivos de una organización, y sus consecuencias. Para ello, se realiza una predicción del futuro, basada en el pasado histórico y en el análisis cuidadoso de los eventos. No reemplaza la experiencia empírica; por el contrario, con frecuencia gran cantidad de información se obtiene a partir de juicios de expertos. Los juicios toman la forma de una distribución de probabilidades, y siguen todas las reglas de la teoría tradicional de probabilidades (Greenberg & Lowrie, 2010).

En este orden de ideas, el método Mosler tiene por objeto la identificación, análisis y evaluación de los factores que pueden influir en la manifestación de un riesgo. Se le aplica con la finalidad de que la información obtenida, permita calcular la clase de riesgo. El método es de tipo secuencial y cada fase del mismo se apoya en los datos obtenidos en las fases que le preceden. Este método comprende un total de cinco (5) fases; las cuales se describen brevemente a continuación:

Fase 1. Definición de Riesgo, tiene por objeto la identificación del riesgo, delimitando su objeto y alcance, para diferenciarlo de otros riesgos. El procedimiento a seguir es mediante la identificación de sus elementos característicos, estos son: a) El bien. b) El daño. Esto quiere decir que se

deben identificar los bienes de la organización, institución o empresa objeto de estudio para posteriormente identificar el daño al cual están expuestos dichos bienes.

Fase 2. Análisis de riesgo: Esta fase tiene como objeto el análisis y ponderación de los criterios que permitirán la evaluación del riesgo, para esto serán considerados los criterios que inciden en la magnitud del daño y los criterios que inciden en la probabilidad. El procedimiento consiste en lo siguiente:

a) Identificación de las variables.

b) Análisis de los factores obtenidos de las variables y ver en qué medida influyen en el criterio considerado, cuantificando los resultados según la escala Mosler o Penta, que se describe a continuación:

- "F" Criterio de función. Las consecuencias negativas o daños pueden alterar de forma diferente la actividad: Muy gravemente 5, Gravemente 4, Medianamente 3, Levemente 2, Muy levemente 1.
- "S" Criterio de sustitución. Los bienes pueden ser sustituidos: Muy difícilmente 5, Difícilmente 4. Sin muchas dificultades 3. Fácilmente 2, Muy fácilmente 1.
- "P" Criterio de Profundidad. La perturbación y los efectos psicológicos que producirían serían de diferente graduación, por sus efectos en la imagen: Perturbaciones muy graves. 5, Perturbaciones graves 4, Perturbaciones limitadas 3, Perturbaciones leves. 2, Perturbaciones muy leves 1.
- "E" Criterio de extensión. El alcance de los daños, según su amplitud o extensión, pueden ser: De alcance internacional. 5, De carácter

nacional. 4, De carácter regional. 3, De carácter local. 2, De carácter individual. 1.

- “A” Criterio de agresión. La probabilidad de que el riesgo se manifieste es: Muy alta 5, Alta 4, Normal 3, Baja 2, Muy baja 1.
- “F” Criterio de vulnerabilidad. La probabilidad de que se produzcan daños es: Muy alta 5, Alta 4, Normal 3, Baja 2, Muy baja 1

Fase 3. Evaluación del riesgo: Esta fase tiene por objeto cuantificar el riesgo considerado, partiendo de cada uno de los datos o valores obtenidos en la fase anterior. Las formulas a emplearse para la cuantificación son las siguientes:

- Importancia del suceso:

I= F x S; donde I = Importancia del suceso

F=Criterio de Función

S= Criterio de Sustitución

- Daños ocasionados:

D= P x E; donde D: Daño ocasionado

P: Profundidad

E: Extensión

Para determinar el daño ocasionado por el riesgo incendio, se procede:

- Carácter del Riesgo:

C= I +D, donde I: Importancia

D= Daños ocasionados

- Probabilidad

Pb= A x V; donde A = Agresión

V= Vulnerabilidad

- Riesgo Esperado

ER= C x Pb; ER= Riesgo Esperado

C = Carácter del Riesgo

Pb= Probabilidad

Fase 4. Clasificación del Riesgo. En esta fase tiene por objeto clasificar el riesgo en función del valor obtenido en la evaluación de la fase anterior los cuales se comparan con la siguiente tabla

VALOR DEL RIESGO ER	**CLASE DE RIESGO**
2-250	Muy pequeño
251-500	Pequeño
501-750	Normal
751-1000	Grande
1001-1250	Elevado

Fase 5. Análisis de Riesgo. En esta fase una vez que se han obtenido y organizado los resultados provenientes de cada una de las fases cumplidas se procede a levantar la tabla de análisis de riesgo que será la base principal para la toma de medidas o estrategias de prevención futura.

Bases legales

La temática enmarcada en la evaluación de la seguridad de los sistemas de información posee un basamento legal establecido en los siguientes instrumentos y legislaciones legales:

Marco legal venezolano:

- Venezuela 2001. Ley Especial Contra Los Delitos Informáticos.

> **Artículo 1:** Objeto de la Ley La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

•Decreto con Fuerza de Ley Mensajes de Datos y Firmas Electrónicas.

> **Artículo 1**.- El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

•Ley Especial Contra los Delitos Informáticos.

> **Artículo 1º** Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley

Normativas:

Serie de Normas ISO 27000

Normas ISO 17799

Legislaciones Internacionales:

- República Dominicana 2007. Ley contra Crímenes y Delitos de Alta Tecnología.

> Artículo l.- Objeto de la Ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

- Chile 1993. Ley Relativa con los Delitos Informáticos.

En junio de 1993 entró en vigencia en Chile la Ley N°19.223, sobre delitos informáticos. La Ley Nº 19.223 tiene como finalidad proteger a un nuevo bien jurídico como es: “la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan”.

La Ley N°19.223, es una ley especial, extra código y consta de 4 artículos, que se enuncian a continuación.

> Artículo 1. “El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo”.
>
> Artículo 2. “El que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio”.
>
> Artículo 3. “El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio”.
>
> Artículo 4. “El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado”.

- Alemania 1986. Ley Contra la Criminalidad Económica.

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos: Espionaje de datos, estafa informática, falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos, alteración de datos; es ilícito cancelar, inutilizar o

alterar datos inclusive la tentativa es punible. Sabotaje informático, destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, Inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa. ŒUtilización abusiva de cheques o tarjetas de crédito.

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, producción del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que, el perjuicio patrimonial que se comete consiste en influir en el resultado de

- Francia 1988. Ley Fraude Informático

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

Œ Acceso fraudulento a un sistema de elaboración de datos (462-2). - En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Œ Sabotaje informático (462-3). - En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Œ Destrucción de datos (462-4). - En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Œ Falsificación de documentos informatizados (462-5). - En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Œ Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

CAPÍTULO III

MARCO METODOLÓGICO

En la presente investigación es de fundamental importancia que los hechos y relaciones que establecen los resultados o los nuevos conocimientos tengan un grado de máxima exactitud y confiabilidad, por esta razón, se presenta un procedimiento ordenado que se sigue para establecer lo significativo de los hechos y fenómenos hacia los cuales está encaminado el interés de la investigación.

Con base en lo anterior, en el presente capítulo se describe el procedimiento empleado en la investigación como vía para el logro de los objetivos propuestos, en función de las características derivadas del problema investigado, destacándose aquí el tipo, diseño y alcance de la investigación, la población y muestra, así como, las técnicas e instrumentos de recolección de datos, las técnicas de análisis de los datos.

Tipo de Investigación

Considerando el proceso de investigación como un conjunto de pasos metódicos y sistemáticos orientados a la solución de problemas por medio del desarrollo de nuevos conocimientos y con propósito de dar respuestas a las interrogantes planteadas; el presente estudio, atendiendo a sus objetivos, se desarrollará con las pautas de la investigación de Campo. En ese sentido, según Arias (2006:52), la investigación de campo “es aquella que consiste en la recolección directamente de los sujetos investigados, o de la realidad

donde ocurren los hechos...” Esto quiere decir que el presente estudio se orientará en la búsqueda y recolecta de la información en la propia organización sometida a estudio, de modo que los datos obtenidos sean de primera mano.

Diseño de la investigación.

El diseño de investigación, no es más que la estrategia general que adoptará el investigador para responder al problema planteado; en atención al diseño, el presente estudio posee un diseño no experimental. En este tipo de diseño, de acuerdo con Hernández (2006:205) “no se construye ninguna situación, sino que se observan situaciones ya existentes, no provocadas intencionalmente en la investigación para quien se realiza”. Esto quiero decir que no existe manipulación de las variable si implicadas, limitándose sólo a la observación del fenómeno objeto de estudio.

Con base en lo antes dicho, en la presente investigación se estudiará una situación ya existente, donde no se tiene el control de las variables como tampoco se puede influir en la relación de las mismas. Es decir, la problemática tratada es una situación presente en la institución estudiada, la cual no fue creada ni influenciada por el investigador.

Alcance de la investigación

Considerando el proceso de investigación como un conjunto de pasos metódicos y sistemáticos orientados a la solución de problemas por medio del desarrollo de nuevos conocimientos y con propósito de dar respuestas a las interrogantes planteadas; el presente estudio, atendiendo a los objetivos planteados se enmarcará en un nivel de tipo explicativo, para lo cual será necesario exponer la razón por la cual se dan cada uno de los aspectos a investigar, esto los sistemas de información y la seguridad de los mismos.

Esta orientación se denomina explicativa, según Díaz (2006:129) porque como su nombre lo indica “su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta se manifiesta este, o por qué dos o más variables esta relacionadas”. Lo anterior indica, que este tipo de estudios buscan la manera de señalar cómo es y cómo se manifiesta el fenómeno de interés, esto teniendo que relacionar las variables medidas.

Técnicas de Recolección de datos

Una vez determinado el tipo de investigación, es necesario escoger los procedimientos que ayuden a recabar óptimamente los datos que solucionarán el problema planteado y con ello permitan el logro de los objetivos; es decir elegir las técnicas e instrumentos que servirán como medio para la conocer los datos necesarios. En ese orden de ideas, se entiende por técnica de recolección de datos, según Arias (2006:67) “el procedimiento o forma particular de obtener datos o información de interés”. Esto quiere decir que es el medio a través del cual se conoce toda la data que permitirá darle respuesta a los objetivos planteados.

En este caso particular, la técnica a emplear será la encuesta; específicamente En este caso particular, la técnica a emplear será la encuesta; la cual según Arias (2006:72) “es una técnica que pretende obtener información que suministra un grupo o muestra de sujetos de sí mismos o en relación con un tema en particular “, en ese orden de ideas, la encuesta será aplicada a la muestra seleccionada, la cual se detalla más adelante.

Instrumento de recolección de Información

Por otra parte, en lo que se refiere al instrumento, según Arias (2006:69) este no es más que “cualquier recurso, dispositivo o formato (en papel o

digital), que se utiliza para obtener, registrar o almacenar información, en este caso, el instrumento a emplear será el cuestionario.

Según Hernández (2006:310) el cuestionario “consiste en un conjunto de preguntas respecto de una o más variables a medir”; en este caso la variable a medir se encuentra relacionada con la seguridad en los sistemas de información del Departamento de Informática de la Universidad sujeta a estudio y el cuestionario a emplear específicamente, es el cuestionario de seguridad facilitado por el Dr. Armando J. Garrido en la cátedra de análisis de riesgos del Programa de especialización en protección industrial.

Método Mosler

El método Mosler tiene por objeto la identificación, análisis y evaluación de los factores que pueden influir en la manifestación de un riesgo. Se le aplicó a Dirección de Informática de la Universidad sujeta a estudio, con la finalidad de que la información obtenida, permita calcular la clase de riesgo. El método es de tipo secuencial y cada fase del mismo se apoya en los datos obtenidos en las fases que le preceden.

Técnicas de Análisis

Una vez recogida y procesada la información, es necesario presentar los resultados de manera adecuada, de forma tal que contribuya a una mejor comprensión y exposición de dichos resultados, en función de los objetivos del trabajo. Según Hernández (2006:408) “actualmente los análisis cuantitativos se realizan mediante computadora u ordenador”. En tal sentido, para este caso en particular se presentaran de manera estadística, tabulada y graficas de barra empleando programas como Microsoft Word y Microsoft Excel.

Población y Muestra

Población

La población según lo establece Hernández (2006:239) “es el conjunto de todos los casos que concuerdan con determinadas especificaciones”. En el caso particular de la presente investigación donde se realizará el análisis de los riesgos presentes en los sistemas de información en cuanto a la seguridad física de la Dirección de Informática de la Universidad sujeta a estudio, la población estuvo conformada por el personal de la Dirección de Informática, cual está conformada de la siguiente manera:

Cuadro Nº1. Población

Departamento	Personal
Desarrollo de Sistema	29
Producción de Sistema	7
Soporte de Sistema	16

Fuente: Elaboración propia (2015)

Muestra

Por otra parte en lo que respecta a la muestra, según Hernández, R (2006:236) esta es “un subgrupo de la población del cual se recolectan los datos y debe ser representativo de dicha población”. Esto quiere decir que de la totalidad de la población, se deberá seleccionar una parte o sección de la misma para ser estudiada.

Con base en lo anterior y considerando la temática tratada, la muestra con la que se trabajará se basará en un muestreo de tipo no probabilístico, el cual de acuerdo con Abascall (2005:69) “no se basa en un proceso de azar sino que es el investigador el que elige la muestra. La elección puede realizarse de diferentes formas sencillas de selección”. En este caso para la selección se tomó una muestra de tipo intencional.

Según Castro (2005:138) la muestra de tipo intencional se refiere a una “decisión hecha con anticipación al comienzo del estudio, según el cual el investigador determina configura una muestra inicial de informantes que poseen un conocimiento generalmente amplio sobre el tópico a indagar.

Teniendo en cuenta lo antes planteado la muestra estará conformada por el personal del departamento de producción de sistemas, dicho departamento es el encargado de administrar y optimizar el uso de los recursos informáticos, custodiar la información y mantener una estructura de datos cónsona con las demandas de los usuarios, así como una red de datos con calidad de enlace, garantizando la operatividad y condiciones de seguridad en el acceso al portal, intranet y sistemas de información desarrollados en la dirección de informática de la universidad sujeta a estudio.

La población en particular está comprendida por un total de sietes (7) empleados, se trabajará específicamente con los administradores de Sistemas los cuales comprende una muestra de 3 personas.

Estrategia Metodológica

Según Delgado de Smith (2013:261) al elaborar un proyecto de investigación se debe aclarar el procedimiento que se tiene previsto transitar. En tal sentido el cuadro técnico metodológico, viene ser la guía que permitirá

exponer de manera detallada los pasos a seguir en el desarrollo de la investigación.

Tal como indica Delgado de Smith (2013:261) la elaboración de este cuadro permite ir descomponiendo a partir de los aspectos generales, los elementos, más concretos que le permiten al investigador acercarse a la realidad objeto de estudio.

Para realizar el cuadro técnico metodológico es necesario hacer la exigida operacionalización de variables, la cual consiste en crear los indicadores que sirvan de categorías o variables para posteriores mediciones, estos indicadores son tomados de los objetivos de la investigación, mencionados en el Capítulo I, y son de suma importancia, a continuación y con base en lo expuesto se presenta el cuadro técnico metodológico de la presente investigación. (Ver cuadro Nº 2)

Cuadro N°2

Cuadro Técnico Metodológico

Objetivo General: Determinar la seguridad de los sistemas de información como mecanismo para la actualización de las medidas de protección en el departamento de informática de una universidad pública.						
OBJETIVO ESPECÍFICO	**VARIABLE**	**DEFINICIÓN**	**INDICADORES**	**ÍTEMS**	**TÉCNICA/ INSTRUMENTO**	**FUENTE**
Analizar los riesgos presentes en los sistemas de información del Departamento de Informática de una universidad pública	Riesgos	La probabilidad de que una amenaza se materialice, utilizando la vulnerabilidad existentes de un activo o grupos de activos, generándoles pérdidas o daños	Fiabilidad Confidencialidad Integridad Disponibilidad	Sección V. Condiciones actuales de protección física: Políticas e instrucciones Sistemas de seguridad y comunicaciones Riesgos y amenazas Acceso a la Instalación	Encuesta/ Cuestionario	Departamento de Producción de Sistemas

Fuente: Gómez, J (2014)

Conocer la seguridad de los sistemas de información con base en los riesgos, debilidades y fortalezas encontradas.	Seguridad de los sistemas	Grado o dimensión de riesgo.	**Clasificación:** • Muy pequeño • Pequeño • Normal • Grande • Elevado	N.A	Método Mosler	Departamento de Producción de Sistemas
Formular estrategias y elementos de seguridad a considerar con base en los resultados obtenidos a partir de la valoración realizada.	Elementos de seguridad	Componentes que contienen, mantienen o guardan información.	• Datos • Sistema e infraestructura • Personal	N.A	N.A	Método Mosler

Fuente: Gómez, J (2014)

CAPÍTULO IV

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS

El propósito del análisis es resumir y comparar las observaciones llevadas a cabo en forma tal que sea posible materializar los resultados de la investigación con el fin de proporcionar respuestas a los interrogantes de la investigación.

En este sentido, Orozco C. y Labrador M. (2007) comentan que las técnicas de procesamiento y análisis de datos corresponde a “la explicación de cómo serán tratados los datos recolectados para hacer la evaluación del fenómeno que representan”. (p.86) Por ello, una vez aplicados los instrumentos para la recolección de la información necesaria y dar respuesta a los objetivos específicos planteados, se procedió a su análisis e interpretación mediante la utilización del método cuantitativo.

En este sentido, el método cuantitativo según Arias, F (2006), destaca, que la estadística ha sido descrita por Lundberg como “... la recopilación, presentación, análisis e interpretación de datos numéricos” (p.127). Teniendo en cuenta lo anterior, en la presente investigación el análisis y presentación de datos obtenidos, se abordó de manera descriptiva, los resultados se agruparon por variables en función de los indicadores hallados la revisión realizada, presentándolos tal como se describe a continuación

Análisis los riesgos presentes en los sistemas de información del Departamento de Informática de una universidad pública.

En esta primera etapa de investigación fue necesario conocer los riesgos presentes en los sistemas de información a fin de dar una definición del riesgo al que se expone el Departamento objeto de estudio, para tal propósito se procedió a conversar con el personal encargado en la administración del sistema.

En ese orden de ideas, mediante una entrevista formal se realizaron un conjunto de preguntas basadas en el cuestionario de seguridad facilitado por el Dr. Armando J. Garrido en la cátedra de análisis de riesgos del Programa de especialización en protección industrial de la Universidad de Carabobo (Ver Anexo Nº 1), los aspectos generados a partir de la entrevista evidenciaron algunas debilidades que se exponen a groso modo a continuación: se conoció en primer lugar las características generales de la instalación sujeta a estudio en cuanto a sus dimensiones de superficie, perímetro, vías de acceso a la misma. Se conoció que la institución en lo que respeta al grado de criminalidad en las áreas circunvecinas, es moderado; se encuentra rodeada principalmente de establecimientos y centros comerciales, entidades bancarias, restaurantes y centros educativos.

En cuanto a las condiciones actuales de protección física se pudo conocer que en un aspecto general están satisfechos con la supervisión de las instalaciones y la eficiencia del personal de seguridad, pese a no ser un personal especialista. Por otra parte, se conoció que algunos equipos de seguridad requieren cambios y consideran preciso la actualización de los sistemas contra incendios. En cuanto a los aspectos de seguridad del sistema también consideran importante la actualización continúa del software de protección pues los mismos tienen firmas de acceso vencidas y los controles de acceso no siempre son respetados debido a la falta de control de cambios de claves.

Con las respuestas obtenidas de esta conversación fue posible identificar los riesgos a los cuales se expone el Departamento quedando establecidos cuatro riesgos específicos: sabotaje con fuga de información, incendios, intrusión y actos vandálicos.

De este modo, a partir de los resultados obtenidos en esta primera etapa de la investigación se procedió a aplicación del Método Mosler con la finalidad de jerarquizar los riesgos y con ellos proceder a al planteamiento de estrategias de seguridad, tal como se muestra seguidamente.

Valoración de la seguridad de los sistemas de información con base en los riesgos, debilidades y fortalezas encontradas.

Una vez identificado los presentes en el Departamento sujeto a estudio, se procedió a la aplicación y desarrollo del método Mosler de análisis de riesgo, el cual tiene como objeto la identificación, análisis y evaluación de los factores que pueden influir en la manifestación de un riesgo, con la finalidad que la información obtenida permita calcular el tipo de riesgo. Se trabajó mediante el desarrollo de cuatro fases: definición de riesgos, análisis del riesgo, evaluación del riesgo y cálculo de la clase de riesgo.

Fase 1ª. Definición del riesgo. Esta fase tuvo como objeto la identificación la identificación del riesgo, delimitando su objeto y alcance, para diferenciarlo de otros riesgos. El procedimiento a seguir se basó en la identificación de sus elementos característicos; estos son: a) El bien. y b) El daño, de los bienes de la organización y de los daños que les pueden afectar, para el desarrollo de la misma se consideraron las respuesta obtenidas a partir de la entrevista realizada al personal encargado de la administración del sistema, el cual como ya se apreció en el primer punto tratado en este capítulo, los riesgos identificados son: sabotaje con fuga de información, incendios, intrusión y actos vandálicos.

Fase 2ª. Análisis del riesgo. Esta fase tiene por objeto analizar y ponderar los criterios, que permitirán la evaluación del riesgo, para esto fue considerado los criterios que inciden en la magnitud del daño y los criterios que inciden en la probabilidad**.** El procedimiento consistió en:

a) Identificación de las variables.

b) Análisis de los factores obtenidos de las variables y ver en qué medida influyen en el criterio considerado, cuantificando los resultados según la escala Mosler o Penta, que se describe a continuación:

- "F" Criterio de función. Las consecuencias negativas o daños pueden alterar de forma diferente la actividad: Muy gravemente 5, Gravemente 4, Medianamente 3, Levemente 2, Muy levemente 1.

- "S" Criterio de sustitución. Los bienes pueden ser sustituidos: Muy difícilmente 5, Difícilmente 4. Sin muchas dificultades 3. Fácilmente 2, Muy fácilmente 1.

- "P" Criterio de Profundidad. La perturbación y los efectos psicológicos que producirían serían de diferente graduación, por sus efectos en la imagen: Perturbaciones muy graves. 5, Perturbaciones graves 4, Perturbaciones limitadas 3, Perturbaciones leves. 2, Perturbaciones muy leves 1.

- "E" Criterio de extensión. El alcance de los daños, según su amplitud o extensión, pueden ser: De alcance internacional. 5, De carácter nacional. 4, De carácter regional. 3, De carácter local. 2, De carácter individual. 1.

- "A" Criterio de agresión. La probabilidad de que el riesgo se manifieste es: Muy alta 5, Alta 4, Normal 3, Baja 2, Muy baja 1.

- “F” Criterio de vulnerabilidad. La probabilidad de que se produzcan daños es: Muy alta 5, Alta 4, Normal 3, Baja 2, Muy baja 1

El Cuadro Nº 3 muestra los criterios, descripción, riesgo y grado estudiados en la fase y cómo fueron distribuidos, se aprecia los valores otorgados cada uno de los riesgos presentes en el Departamento objeto de estudio.

Cuadro Nº3. Fase 2 del análisis de riesgo

CRITERIO	DESCRIPCIÓN	RIESGO	GRADUACIÓN				
			5	4	3	2	1
DE MAGNITUD	FUNCIÓN	INCENDIO	X				
	SUSTITUCIÓN		X				
	PROFUNDIDAD			X			
	EXTENSIÓN			X			
	FUNCIÓN	SABOTAJE CON FUGA DE INFORMACIÓN		X			
	SUSTITUCIÓN			X			
	PROFUNDIDAD				X		
	EXTENSIÓN			X			
	FUNCIÓN	INTRUSIÓN		X			
	SUSTITUCIÓN			X			
	PROFUNDIDAD				X		
	EXTENSIÓN			X			
	FUNCIÓN	ACTOS VANDÁLICOS	X				
	SUSTITUCIÓN		X				
	PROFUNDIDAD			X			
	EXTENSIÓN			X			
DE PROBABILIDAD	AGRESIÓN	INCENDIO	X				
	VULNERABILIDAD			X			
	AGRESIÓN	SABOTAJE CON FUGA DE INFORMACIÓN	X				
	VULNERABILIDAD			X			
	AGRESIÓN	INTRUSIÓN			X		
	VULNERABILIDAD					X	
	AGRESIÓN	ACTOS VANDÁLICOS			X		
	VULNERABILIDAD					X	

Fuente: Gómez, J (2015)

Fase 3ª. Evaluación del Riesgo

Partiendo de cada uno de los datos o valores obtenidos en las tablas anteriores se procedió a cuantificar el riesgo esperado teniendo en cuenta los criterios planteados anteriormente. A continuación se muestra un cálculo tipo que serán posteriormente presentados en la tabla de análisis de riesgo.

- Importancia del suceso:

I= Fx S; donde I = Importancia del suceso

F=Criterio de Función

S= Criterio de Sustitución

Para la determinación de la importancia del riesgo incendio se obtiene:

I= 5 x 5 = 25

- Daños ocasionados:

D= P x E; donde D: Daño ocasionado
P: Profundidad
E: Extensión

Para determinar el daño ocasionado por el riesgo incendio, se procede:

D= 4 x 4 = 20

- Carácter del Riesgo:

C= I +D, donde I: Importancia

D= Daños ocasionados

Para determinar el Carácter del Riesgo para el riesgo incendio, se procede:

C= 25 + 20= 45

- Probabilidad

  Pb= A x V; donde A = Agresión

  V= Vulnerabilidad

Para determinar la Probabilidad del riesgo incendio, se procede:

Pb= 5x4 =20

- Riesgo Esperado

  ER= C x Pb; ER= Riesgo Esperado

  C = Carácter del Riesgo

  Pb= Probabilidad

Para determinar el Riesgo Esperado del riesgo incendio, se procede:

ER= 45 x 20 = 900

Fase 4ª Clasificación del Riesgo

Una vez que se han obtenido los valores de la evaluación se procedió a clasificar el riesgo en función de dichos valores, para ello se tuvo en cuenta la siguiente tabla de la cual se tomaron los resultados y vaciaron en la tabla resumen del Análisis de Riesgo.

VALOR DEL RIESGO ER	CLASE DE RIESGO
2-250	Muy pequeño
251-500	Pequeño
501-750	Normal
751-1000	Grande
1001-1250	Elevado

Fase 5ª Análisis de Riesgo

Una vez que se han obtenido y organizado los resultados provenientes de cada una de las fases cumplidas se procede a levantar la tabla de análisis de riesgo que será la base principal para la toma de medidas o estrategias de prevención futura, para el caso particular del área sometida a estudio el análisis de riesgo fue el siguiente.

Cuadro Nº4. Análisis de Riesgo

CRITERIOS			RIESGOS			
			INCENDIO	SABOTAJE INFORMATICO Y FUGA DE INFORMACIÓN	INTRUSIÓN	ACTOS VANDÁLICOS
DE MAGNITUD	Función	F	5	5	5	4
	Sustitución	S	5	5	5	3
	Importancia de Suceso	I=F x S	25	25	25	12
	Profundidad	P	5	5	5	4
	Extensión	E	4	5	5	3
	Daños Ocasionados	D=P x E	20	25	25	12
	CARÁCTER DEL RIESGO	C= I + D	45	50	50	24
DE PROBABILIDAD	Agresión	A	5	5	3	3
	Vulnerabilidad	V	4	4	3	3
	PROBABILIDAD	Pb= A x V	20	20	9	9
Valor del riesgo (Riesgo Esperado)		ER= CxPb	900	1000	450	216
CLASIFICACIÓN DEL RIESGO			GRANDE	ELEVADO	PEQUEÑO	MUY PEQUEÑO

Fuente: Gómez, J (2015)

Con base en estos resultados la clasificación del riesgo de la variable Incendio, se cuantifica en900 puntos dando un criterio de evaluación 751-1000, considerando una clase del riesgo Grande. En cuanto a la variable sabotaje informático y fuga de información, se cuantifico el mismo, obteniendo1000 puntos, dando un criterio de evaluación751-1000, considerando una clase del riesgo Grande.

En este mismo orden en cuanto a la variable Intrusión, su cuantificación del riesgo fue de 450 puntos, con un criterio de evaluación 251-500, considerado en una clase del riesgo Pequeño. En la variable Actos vandálicos su cuantificación fue de 216 puntos, con un criterio de evaluación 2-250, considerado en una clase del riesgo Muy pequeño.

Estrategias de seguridad a considerar con base en los resultados obtenidos a partir de la valoración realizada.

Tal como puede apreciarse en los resultados obtenidos a través de la aplicación del método Mosler de análisis de riesgo, la institución sometida a estudio presenta un riesgo elevado relacionado con el sabotaje informático fuga de información. En ese sentido, debe considerarse que el impacto y las consecuencias posteriores a un incidente de fuga de información, es uno de los aspectos que mayor preocupación despierta en las organizaciones, puesto que la filtración de información puede dañar su imagen pública, además de generar desconfianza e inseguridad en el público en general y generar otras consecuencias a terceros, como en el caso de que la información filtrada haga referencia a usuarios o clientes.

Es por ello que se hace necesario para la organización sometida a estudio considerar algunos aspectos extras relacionados con este riesgo de manera de minimizar el mismo. En ese orden de ideas, se sabe que la prevención del sabotaje y la fuga de información pasa por la aplicación de

medidas de seguridad desde tres puntos de vista: técnico, organizativo y legal, es así, como con base en esto se exponen algunas medidas que son consideradas estrategias, las cuales pueden aportar valor al sistema de seguridad actual de la institución:

Cuadro Nº5. Medidas sugeridas para minimizar riesgos sabotaje informático y fuga de información

Medidas Organizativas	Medidas Técnicas	Medidas legales
Buenas practicas	Control de acceso e identidad	Solicitud de aceptación de política de seguridad
Política de seguridad	Soluciones anti-malware y anti-fraude Seguridad perimetral y protección de las comunicaciones	Solicitud de aceptación de política de confidencialidad Otras medidas de carácter disuasorio en base a legislación
Procedimientos	Control de contenidos y control de tráfico Copias de seguridad	Solicitud de aceptación de política de seguridad
Clasificación de la información, establecimiento de roles y niveles de acceso	Control de acceso a los recursos Actualizaciones de seguridad y parches	
Formación e información interna	Otras medidas de seguridad derivadas del cumplimiento de legislación Gestión de eventos e inteligencia de seguridad	
Sistema de gestión de seguridad de la información		

Fuente: Gómez, J (2015)

Además de las buenas prácticas y la formación es necesario contar con procedimientos y establecer el conjunto de pautas y obligaciones para los

trabajadores en el ámbito de la seguridad, mediante el establecimiento de políticas que indiquen claramente cuáles son los límites dentro de los cuales deberán desempeñar su actividad y por otro lado, los procedimientos para aquellas actividades de especial importancia o riesgo, de manera que se sigua un proceso controlado y las tareas se realicen de la forma más segura posible.

Aunado a esto, además de la formación, las buenas prácticas y las políticas, es necesario ir más allá, con el propósito de incorporar un nivel adicional de disuasión, a fin de evitar prácticas indebidas o actividades malintencionadas dentro de las organizaciones.

Por otra parte, en cuanto al riesgo relacionado con la posibilidad de incendio, se hace necesario determinar un plan de prevención y de emergencia de incendios adecuados a las necesidades de la organización sometida a estudio. En tal sentido, las estrategias que se estiman como posibles medidas que permitirán el refuerzo de los sistemas contra incendio con los que cuenta actualmente la institución sometida a estudio, son los siguientes:

Crear un Plan de Prevención y Emergencia en el cual sean considerados los siguientes aspectos:

1 La identificación y la evaluación de los riesgos potenciales posibles.

2 El inventario de los medios de protección existentes.

3 El establecimiento de la organización más adecuada de las personas que deben intervenir, definiendo las funciones a desarrollar por cada una de ellas en el transcurso de las diferentes emergencias posibles, estableciendo la línea de mando y el procedimiento para iniciar las actuaciones cuando se produzca la alarma.

4 La Implantación del Plan de Emergencia, esto es, su divulgación general entre los empleados.

Este plan deberá a su vez deberá cumplir con algunos aspectos que permitirán el éxito del mismo, tales aspectos son: formularse por escrito, tener aprobación de la máxima autoridad de la Empresa, ser difundido ampliamente para su condimento general, ser enseñado y verificado su aprendizaje y ser practicado regularmente a través de “Simulacros”.

Adicional a lo anterior se considera necesario que la institución cuenten con una organización interna, comúnmente existen las llamadas brigadas, las cuales permiten prever y en su caso atender cualquier contingencia derivada de emergencia, siniestro o desastre. Las brigadas son grupos de personas organizadas y capacitadas para emergencias. Los integrantes de las mismas serán responsables de combatirlas de manera preventiva o ante eventualidades de alto riesgo que ocurran en la empresa y cuya función está orientada a salvaguardar a las personas, sus bienes y el entorno de los mismos.

Estas brigadas obedecen a un layout organizacional y funcional que debe ser conocido por todos, realizan simulacros y entrenan al personal en el uso de extintores, así como, a conocer la ruta de evacuación. En general para lograr una estrategia que refuerce la seguridad ante un incendio y minimice el riesgo del mismo, a lo anteriormente expuesto deberá sumarse: la capacitación de los empleados en el plan de emergencias, así como la capacitación en la atención en primeros auxilios médicos, la creación y disposición de carteles con consignas para informar a los proveedores y visitantes de las instalaciones sobre actuaciones de prevención de riesgos y el comportamiento a seguir en caso de emergencia.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

En relación con los riesgos presentes en los sistemas de información del Departamento de Informática de una universidad pública, se concluye que los mismos se encuentra relacionados principalmente a cuatro aspectos o riesgos a considerar: incendio, sabotaje informático y fuga de información, intrusión y actos vandálicos.

Con respecto a estos riesgos, se entiende que la causa principal de los mismos tiende a ser organizativas o técnicas, por lo general, implican la ausencia de algún tipo de medida de seguridad, procedimiento, herramienta, entre otros. Tal ausencia, supone la falta de control y esta aumenta de forma significativa la probabilidad de que se produzca un incidente como los mencionados.

De allí, se concluye que la aplicación de un análisis de riesgo es de suma importancia para determinar para cada una de esas amenazas, dejando en evidencia aquella con mayor vulnerabilidad, si bien estas pueden ser vistas como el resultado de una gestión deficiente, la falta de formación y buenas prácticas, la ausencia de políticas y procedimientos o la no aplicación de mecanismos de disuasión. Estas causas resultan habituales y suficientes para facilitar o desencadenar un incidente relacionados con incendio, sabotaje informático y fuga de información, intrusión y actos vandálicos, por lo cual ameritan atención.

Siguiendo el orden de los objetivos de investigación, en lo que respecta a la seguridad de los sistemas de información con base en los riesgos, debilidades y fortalezas encontradas, una vez realizado el análisis de riesgo basado en la aplicación del Método Mosler se concluye que la seguridad de

estos sistemas presenta vulnerabilidad en los riesgos relacionados con incendio y sabotaje informático y fuga de información, ya que en estos dos los resultados arrojaron un valor del riesgo que clasificó a los mismos en grande y elevado respectivamente.

En la práctica es difícil separar las causas organizativas y técnicas de tales riesgos, puesto que cada vez están más relacionadas, debido al uso intensivo de las tecnologías de la información dentro de las organizaciones para cualquier actividad, incluida la gestión de la seguridad, pero aun así, es importante diferenciarlas, de cara a diseñar medias y detectar vulnerabilidades y mejoras.

Es por ello que al concluir sobre este aspecto, hay que orientar el tratamiento de esta vulnerabilidad a una gestión del Riesgo apoyada en el Análisis de Riesgos conforme al proceso, que permite identificar, estudiar y evaluar a través delas diferentes variables implicadas, los potenciales eventos que afecten los objetivos de una organización, y sus consecuencias.

Por su parte, en lo referentes a las estrategias de seguridad a considerar con base en los resultados obtenidos a partir de la valoración realizada, se concluye que es necesario en cuanto al riesgo por sabotaje informático y fuga de información tomar medidas de refuerzo en cuanto a los aspectos organizativos, técnicos y legales, de manera de que se sigua un proceso controlado y las tareas se realicen de la forma más segura posible.

En cuanto a las estrategias de seguridad relacionadas con el riesgo de incendio, se concluye en la necesidad de crear un plan de Prevención y Emergencia, que se refuerce con medidas de capacitación al personal y formación de brigada de emergencia.

Es de acotar que en el proceso de decisión hacia la solución de estas amenazas o riesgos, la organización puede priorizarla implantación de las

medidas de seguridad sobre lavase de criterios económicos, temporales, entre otros. Esto implica que a través del análisis y gestión de los riesgos se consiga un enfoque global e integrado de la seguridad del sistema de información. No obstante, debido a la diversidad y variabilidad de las amenazas a los que están expuestos los sistemas de información, ningún sistema de seguridad elimina completamente la posibilidad de verse afectado poruña amenaza al sistema.

Es por lo anterior, que la seguridad de un sistema de información de cualquier institución, departamento u organización se puede conseguir mediante la implantación de las medidas oportunas que contribuyan a disminuir los riesgos producidos por las amenazas que le puedan afectar. Estas medidas, que pueden ser organizativas o tecnológicas, permiten crear un entorno seguro para los datos, la información, las aplicaciones y los sistemas que los soportan.

Recomendaciones

- Es indispensable una administración de riesgos concientizada y no verla como un proceso de mejora.
- Es necesario tener conciencia de la administración de riesgos como un sector clave, porque de ella depende la información que resguarda la institución, la cual se emplea para llevar a cabo la misión y visión, así como los servicios o productos que se brinden.
- En la actualidad la industria de seguridad ofrece un buen número de soluciones de seguridad en forma de productos y servicios, entre los que destacan aquellos destinados a la gestión del ciclo de vida de la información o los que están destinados específicamente a evitar la fuga de información, por lo que se recomienda, de ser necesario, buscar asesoría al respecto de manera de ondear más profundamente

en los aspectos de seguridad y las necesidades de la institución sometida a estudio.

LISTA DE REFERENCIAS

Abascal, Elena (2005) **Análisis de Encuestas.** ESIC Editorial, Madrid, España.

Abreu, A (2001)**Principios de Metodología de la Investigación.** Tercera Edición. Editorial Renace. Buenos Aires.

Andreu, Ricart (1991)**Estrategia y Sistemas de Información**. Mc Graw-Hill, Madrid

Arias, Fidias (2006) **El proyecto de investigación**. Editorial Episteme. 5° Edición. Caracas Venezuela.

Barcos, Santiago (2008) **Reflexiones acerca de los sistemas de información universitarios ante los desafíos y cambios generados por los procesos de evaluación y acreditación.** Material didáctico de la cátedra de Administración de la Educación y de las Instituciones Educativas, Facultad de Humanidades y Ciencias de la Educación de la UNLP, La Plata.

Bran, T (2010)**Análisis y seguridad de los sistemas de información**. Editorial Mc Graw Hill, México.

Bringas, María (2011)**Las estadísticas en educación, elemento clave en el diseño de políticas educativas. Una propuesta para mejorar el Sistema de Información Básica de la Educación Normal (SIBEN).**

Cedeño, Marcos (2008) **Seguridad de los sistemas de Información**. Documento en línea disponible en: http://campuscurico.utalca.cl/espinos/2-Sistemas_informaciOn.pdf

De Freitas (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

Decreto con Fuerza de Ley Mensajes de Datos y Firmas Electrónicas. Gaceta Oficial Nº 37.076. Enero 2001

Delgado de Smith, Yamile (2013) **La investigación social en proceso: ejercicios y respuestas**. 2ª reimpresión de la 3º edición. Dirección de medios y publicaciones de la Universidad de Carabobo.

Hernández, Fernández y Baptista, (2006). **Metodología de la Investigación**. 4ª Edición. Editorial Mc Graw Hill.

Huerta, Antonio (2008) "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later..

Ibarra, M (2008) **Administración y Seguridad de los Sistemas de Información**. México, Prentice Hall Internacional.

Ley Especial Contra Los Delitos Informáticos 2001.

Ley contra Crímenes y Delitos de Alta Tecnología.República Dominicana 2007.

Ley Relativa con los Delitos Informáticos. Alemania 1986

Ley Fraude Informático.Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático. Francia

Martínez, Albert (2006**) La seguridad de los sistemas de información en Radiología**. Documento en línea disponible en:http://www.conganat.org/SEIS/is/is45/IS45_109.pdf

Mendoza, Rosendo A. (2010) S**istema de gestión para la seguridad de la información caso: Centro de tecnología de información ycomunicación del decanato deciencias y tecnología – UCLA.** Trabajo de grado presentado como requisito parcial para optaral grado de Magíster Scientiarum en Ciencias de la Computación. Universidad Centroccidental “Lisandro Alvarado” Decanato de Ciencias y TecnologíaMaestría en Ciencias de la Computación.

Mifsud, Elvira (2012) **Introducción a la seguridad informática.**http://recursostic.educacion.es/observatorio/web/es/software/software-gen nera 1040-introduccion-a-la-seguridad-informatica?showall=1

Montesino (2013) **Gestión automatizada e integrada de controles de seguridad informática**. Tesis presentada ante la Universidad de las Ciencias Informáticas (UCI), La Habana, cuba

Norma ISO/IEC. ISO/IEC 27001: Information technology - Security techniques - Information security management systems – Requirements. 2005. : International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

Payren, X (2004) **Sistemas de información. Principios y riesgos.** Editorial Mc. Graw-Hill. Madrid. España.

Peña, De Santiago (2006) **Principios generales de los Sistemas de Información**. Editorial P. Hall. Madrid. España

Peralta, José (2008)**Sistema de información en las organizaciones**. Pirámide editores. Santiago de Chile.

Pérez y Campanero (2010) **La gestión de la seguridad en los sistemas de información y de las comunicaciones.** Telefonía. Madrid España

Ruiz (2010**) Un modelo para el desarrollo de sistemas de detección de situaciones de riesgo capaces de integrar información de fuentes heterogéneas.**

Sánchez, Fabio (2009) **Sistema de información y tecnologías de la información**. Documento en línea disponible en: http://www.inegi.org.mx/est/contenidos/espanol/rutinas/ept.asp?t=apin80&s=est&c=14150

Serie de Normas ISO 27000.Security home. URL: http://www.iso27001security.com/index.html. (Consulta:enero 15, 2014)

Soler, J (2009) **Sistemas de Información para la administración**, Editorial DIANA, México.

Universidad Tecnológica Nacional de Buenos Aires, Argentina (2008); Modelo de Política de Seguridad de la Informaciónpara Organismos de la Administración Pública Nacional publicado por la Oficina Nacional de Tecnología de Información (ONTI) de Argentina.

ANEXOS

Anexo 1.

UNIVERSIDAD DE CARABOBO
FACULTAD DE CIENCIAS ECONOMICAS Y SOCIALES
DIRECCION DE ESTUDIOS PARA GRADUADOS.
PROGRAMA DE ESPECIALIZACION EN PROTECCION INDUSTRIAL.
CATEDRA. ANALISIS DE RIESGOS.
DR. ARMANDO J. GARRIDO

CUESTIONARIO DE SEGURIDAD

I. Datos generales de la instalación:

Fecha de estudio:
_____

Nombre de la instalación:
_____
_____
_____

Ubicación:
_____
_____
_____

Antigüedad de la instalación:
_____

Encuestado:
_____

Cargo:

_____
__

¿Cuándo se llevo a cabo la ultima inspección de seguridad en la instalación?

_____

_____
_____

Analista:

II. Descripción general de la instalación:

- Descripción general:

(Facilitar mapa del área y plano de la instalación):

_____

_____
_____

_____
_____

_____
_____

_____
_____

- Descripción del área de ubicación de la instalación:

_____

_____
_____

_____
_____

- Superficie de la instalación en metros cuadrados o hectáreas: _____
_____
_____

a. Ocupado:
_____

b. Vacío:
_____

- Descripción del terreno (topografía), donde esta ubicada la instalación: _____
_____
_____
_____
_____
_____
_____
_____

- Descripción de los terrenos que rodean el perímetro de la instalación, indicando propietario y uso de las mismas:

a. Norte:

_____
_____
_____

b. Sur:

_____
_____
_____

c. Este:

_____
_____
_____

d. Oeste:

_____

- Descripción de la vegetación (árboles, arbustos) próxima a la(s) cerca(s) del perímetro de la instalación:

_____

a. Dentro del perímetro:

_____
_____
_____
_____
_____

b. Fuera del perímetro:

_____

_____
_____
_____
_____

c. Entre las cercas del perímetro: _____

_____
_____
_____
_____

- Descripción de todas las vías, carreteras, caminos o muelles que dan acceso a pie, en vehículo, o cualquier otro medio a la instalación: _____

_____
_____
_____
_____
_____
_____

III. Entorno:

- Evaluación del grado de criminalidad en áreas circunvecinas, nivel socio económico de la población, tendencias y proporción de desempleo en dichas áreas: _____

_____
_____

- ¿Hay quejas o temas controversiales en el entorno relacionados con las actividades de la instalación?

_____
_____
_____
_____

IV. Funciones y características:

- Describir brevemente el proceso productivo de la empresa, bajo los siguientes aspectos:

a. Cargos:

_____
_____
_____
_____

b. Clasificación:

_____
_____
_____
_____

c. Describir y obtener un diagrama del proceso:

_____
_____
_____
_____
_____

- Descripción del tipo y numero de edificaciones: _____
_____
_____
_____
_____
_____
_____
_____
_____
_____

- ¿Es factible una expansión? _____
_____
_____

- Existen en el entorno otras instalaciones para mantener el proceso operativo en caso de contingencia? _____
_____
_____
_____
_____

- ¿Qué servicio externos, como energía eléctrica, agua, entre otros, son esenciales para las operaciones del lugar? _____

a. ¿Dónde están ubicados? _____

b. ¿Cómo son suministrados? _____

_____

c. ¿Qué sucedería en caso de falla? _____

d. ¿Existe algún respaldo? _____

V. Condiciones actuales de protección física:

Políticas e instrucciones

- ¿Esta satisfecha la supervisión de la instalación con las medidas de protección física y sus procedimientos? De no ser asi, ¿qué mejoras generales le gustaría ver? _____

_____

_____

_____

_____

- ¿Cómo evalúa la eficiencia de? (excelente – buena – regular - mala)

a. Personal de seguridad: _____
_____
_____

b. Los vigilantes (propios o contratados): _____
_____
_____

- ¿Cómo esta entrenado y equipado el personal de seguridad? _____
_____
_____
_____
_____

a. ¿Qué técnicas utilizan para reprimir o interrumpir altercados o peleas? _____
_____
_____
_____

b. ¿Cuáles son los diferentes niveles de fuerza utilizados para protegerse y proteger a los empleados? _____
_____
_____

- ¿Los vigilantes están familiarizados con las instalaciones y el área circundante? ____

_____
_____

- ¿Existen programas para capacitar al personal de seguridad en los procedimientos de seguridad, con programas frecuentes de capacitación o con la publicación de boletines regulares? _____

_____
_____

_____
_____

_____
_____

- ¿Se llevan a cabo simulacros de seguridad, incendio, terremoto, dentro de la instalación? _____

_____
_____

- ¿Cómo se lleva a cabo el control de llaves y cerraduras? _____

_____
_____

Perímetro e iluminación:

- ¿Esta rodeado el lugar por una barrera perimetral (cercas, paredes, edificios)? De ser asi, describa:

    a. Longitud:

    _____
_____
_____

    b. Tipo (malla ciclón, alambre de púas, paredes): _____
_____
_____

    c. Altura:

    _____
_____
_____

    d. Distancia entre el doble perímetro: _____
_____
_____

- ¿Existen puntos no autorizados de entrada al perímetro de la instalación como alcantarillas, drenajes, tuberías, entre otros, ?

_____
_____
_____
_____

- ¿Esta adecuadamente iluminado el perímetro de la instalación? ¿El encendido es automático? Describe como es la iluminación: señala las áreas que no están adecuadamente iluminadas. _____
_____
_____
_____

- ¿Qué tipo de iluminación tienen las oficinas? _____
_____
_____

- ¿Esta el sistema de iluminación de la instalación conectada a la planta eléctrica de emergencia?. _____-
_____
_____
_____

- ¿Existen áreas de estacionamiento de vehículos dentro del perímetro de la instalación?
_____
_____
_____

a. ¿Existen áreas de estacionamiento para la empresa? _____

_____
_____

b. ¿Existen áreas de estacionamiento para visitantes? _____
_____
_____

c. ¿El área de estacionamiento periférico crea conflicto con las áreas residenciales o cercanas? _____
_____
_____

d. ¿Las vías de los estacionamientos son largas? _____
_____
_____

e. ¿Dónde se encuentran las áreas de carga y descarga? _____
_____
_____

f. ¿Existen pasos peatonales? _____
_____
_____

g. ¿Existen y se mantienen señalizaciones apropiadas de índices de velocidad y pare? _____
__

_____
_____

h. ¿Cómo esta instalada la señalización?
_____
_____
_____

i. ¿La señalización es clara, de tamaño razonable y colocada en sitios de fácil visualización?
_____
_____
_____

Control de Perdidas / Salida de Materiales

- ¿Existe un área de almacenamiento de equipos? ¿Cómo impide el personal de protección que salgan equipos ilegalmente?
  _____
_____
_____
_____
_____
_____
_____

- ¿En caso de pérdida, esta se reporta? ¿De que forma? ¿A quien?
  _____
  _____
  _____

Acceso a la instalación:

- Describe todos los puntos de entrada en el perímetro.
    a. Ubicación:

_____

    b. Tipo:

_____

    c. Altura:

_____

    d. Ancho:

_____

    e. Condiciones:

_____

    f. Vigilado o no vigilado por personas: si ( ) no ( )
        - ¿Cuándo?

_____

        - ¿Por quien?

_____

    g. ¿Cuál es el horario? ¿Cuánto tiempo permanece abierta? _____

_____

_____

    h. Medidas de seguridad adicionales, asociadas (policías acostados, barreras, cadenas, supervisión con CCTV, control de registro de entrada y salida por fotografías):

_____
_____
_____
_____

- ¿Qué sistema se utiliza para abrir o cerrar los puntos de acceso? _____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

- Existen señales o letreros alrededores del perimetro de la instalación que adviertan que se trata de un área vigilada y que esta prohibido el acceso no autorizado? _____

_____
_____
_____
_____

- ¿Los vigilantes se registran antes de llegar a la instalación? _____

_____
_____

- ¿Cómo se verifica que después de las horas laborales solo quedan en el lugar las personas debidamente autorizadas? _____

_____
_____

- ¿Cómo es el acceso al techo? _____

_____
_____

a. ¿La estructura de la instalación permite un acceso rápido y de fácil mantenimiento?

_____
_____
_____

- ¿Están definidos los sitios formales de reunión? _____

_____
_____

- ¿Las áreas informales de reunión están visibles? _____

- ¿Los trabajadores utilizan las áreas externas a la edificación como sitio informal de reunión ¿ _____ _

- ¿Existe un área destinada para los casilleros de los empleados? _____
_____ _____
_____ _____

- ¿Dónde están ubicados los baños? _____
_____ _____

- ¿Existen rampas, pasamanos y cambios de nivel aceptables? _____
_____ _____

- ¿Los corredores y pasillos son lo suficientemente anchos para permitir sillas de ruedas sin interrumpir el paso? _____

_____
_____

¿Los marcos de puertas crean puntos ciegos peligrosos? _____
_____
_____

- ¿La entrada principal es despejada, es fácilmente accesible? _____
_____
_____

- ¿Las oficinas administrativas tienen líneas claras del sitio, de las áreas de recreación, reunión y estacionamiento? _____
_____
_____

- ¿El paisajismo, las puertas y/o cercas, permiten la observación hacia las áreas circundantes? _____
_____
_____

- ¿Existen puertas / salidas de emergencias? _____

_____
_____

- ¿Dónde están los cuartos de electricidad o equipo mecánico? _____

_____
_____
_____
_____

- ¿Existen computadoras u otros equipos costoso dentro de las instalaciones? _____

_____
_____

a. ¿Están asegurados, protegidos y vigilados? _____

Sistemas de Seguridad / Comunicaciones:

- ¿Existen sistemas de alarma, detección de intrusos, CCTV?: _____

_____
_____
_____
_____
_____
_____

_____
_____

a. ¿Qué bienes protegen?
_____
_____
_____

b. ¿Dónde están ubicados?
_____
_____
_____

c. ¿Son efectivos día y noche?
_____
_____
_____

d. ¿Impiden, detectar o rastrean el incidente?
_____
_____
_____
_____

- ¿El CCTV opera continuamente?
  _____
- ¿Los videos son analizadas y archivados?
  _____
- ¿Existen alarmas de pánico?
  _____

a. ¿Dónde están ubicadas? _____

b. ¿Están integradas con los demás sistemas de seguridad y protección? _____

_____

- ¿Existen sistemas de comunicaciones?

a. Están integrados con los demás sistemas de seguridad y protección? _____

_____

- ¿Dónde han sido más efectivos los sistemas de seguridad? _____

_____

a. ¿Cuándo y por que han fallado? _____

_____

_____

b. ¿Cuál es la frecuencia de mantenimiento de estos sistemas de seguridad?

_____
_____
_____
_____

VI. Riesgos y Amenazas:

Identificar las amenazas / riesgos a los cuales esta expuesta la instalación y la frecuencia de ocurrencia? ¿Están aumentando? _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

RIESGOS	AMENAZAS	BIENES VALOREN CRITICIDAD	NIVEL DE IMPACTO (bajo,medio, alto,critico)	PROBABILIDADES OCURRENCIA (nula,poco, probable, muy probable)	FRECUENCIA
HOMICIDIOS					
LESIONES					
DAÑOS PROPIEDAD (vandalismo, bombas)					
DROGAS					
HURTO					
INGRESO ARMAS					
ROBO					
SECUESTRO					
EXTORSION					
OTROS					

- ¿Se han formulado amenazas por parte de los empleados? _____

_____
_____

- ¿Han ocurrido incidentes de violencia dentro de las instalaciones? _____

_____
_____

- ¿Se han reportado hechos de violencia reciente a las propiedades por parte de los empleados? _____

_____
_____

- ¿Existe una política clara y publicada con relación a intimidación o amenazas?

  _____

_____
_____

¿Existen procedimientos de reporte de señales de violencia? _____

_____
_____

- ¿Existen en el lugar donde se ubica la instalación bandas o alteradores del orden? _____

_____
_____

- ¿Existen entrenamientos sobre técnicas de manejo de ira, alivio del estrés, mediación y prevención de la violencia para los empleados? _____
_____
_____
_____
_____

- ¿Se analiza la existencia de empleados con síntomas de depresión o tendencias suicidas? _____
_
_____
_____

- ¿Los empleados reciben capacitación en autoprotección personal? _____
_____
_____
_____
_____

- ¿Se llevan a cabo procesos de búsqueda de drogas ilícitas dentro de las instalaciones de la empresa? _____

_____
_____

- ¿Se practican detecciones de metales a los empleados al ingresar a las instalaciones de empresa?
  _____
_____
_____