CARTA DE AUTORIZACIÓN DE LOS AUTORES

(Licencia de uso)

Bogotá, D.C., Enero 17 de 2014

Señores
Biblioteca Alfonso Borrero Cabal S.J.
Pontificia Universidad Javeriana
Cuidad

Los suscritos:

Felipe Bayona Borrero , con C.C. No 1020746851

, con C.C. No

, con C.C. No

En mi (nuestra) calidad de autor (es) exclusivo (s) de la obra titulada:
Guía Metodológica para la Administración de la Seguridad Física de la Información en Pymes

(por favor señale con una "x" las opciones que apliquen)

Tesis doctoral [ ] Trabajo de grado [X] Premio o distinción: Si [ ] No [X]

cual:

presentado y aprobado en el año 2013 , por medio del presente escrito autorizo (autorizamos) a la Pontificia Universidad Javeriana para que, en desarrollo de la presente licencia de uso parcial, pueda ejercer sobre mi (nuestra) obra las atribuciones que se indican a continuación, teniendo en cuenta que en cualquier caso, la finalidad perseguida será facilitar, difundir y promover el aprendizaje, la enseñanza y la investigación.

En consecuencia, las atribuciones de usos temporales y parciales que por virtud de la presente licencia se autorizan a la Pontificia Universidad Javeriana, a los usuarios de la Biblioteca Alfonso Borrero Cabal S.J., así como a los usuarios de las redes, bases de datos y demás sitios web con los que la Universidad tenga perfeccionado un convenio, son:

AUTORIZO (AUTORIZAMOS)	SI	NO
La conservación de los ejemplares necesarios en la sala de tesis y trabajos de grado de la Biblioteca.	X	
La consulta física (sólo en las instalaciones de la Biblioteca)	X	

AUTORIZO (AUTORIZAMOS)	SI	NO
La consulta electrónica – on line (a través del catálogo Biblos y el Repositorio Institucional)	X	
La reproducción por cualquier formato conocido o por conocer	X	
La comunicación pública por cualquier procedimiento o medio físico o electrónico, así como su puesta a disposición en Internet	X	
La inclusión en bases de datos y en sitios web sean éstos onerosos o gratuitos, existiendo con ellos previo convenio perfeccionado con la Pontificia Universidad Javeriana para efectos de satisfacer los fines previstos. En este evento, tales sitios y sus usuarios tendrán las mismas facultades que las aquí concedidas con las mismas limitaciones y condiciones	X	

De acuerdo con la naturaleza del uso concedido, la presente licencia parcial se otorga a título gratuito por el máximo tiempo legal colombiano, con el propósito de que en dicho lapso mi (nuestra) obra sea explotada en las condiciones aquí estipuladas y para los fines indicados, respetando siempre la titularidad de los derechos patrimoniales y morales correspondientes, de acuerdo con los usos honrados, de manera proporcional y justificada a la finalidad perseguida, sin ánimo de lucro ni de comercialización.

De manera complementaria, garantizo (garantizamos) en mi (nuestra) calidad de estudiante (s) y por ende autor (es) exclusivo (s), que la Tesis o Trabajo de Grado en cuestión, es producto de mi (nuestra) plena autoría, de mi (nuestro) esfuerzo personal intelectual, como consecuencia de mi (nuestra) creación original particular y, por tanto, soy (somos) el (los) único (s) titular (es) de la misma. Además, aseguro (aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos de la Tesis o Trabajo de Grado es de mí (nuestro) competencia exclusiva, eximiendo de toda responsabilidad a la Pontifica Universidad Javeriana por tales aspectos.

Sin perjuicio de los usos y atribuciones otorgadas en virtud de este documento, continuaré (continuaremos) conservando los correspondientes derechos patrimoniales sin modificación o

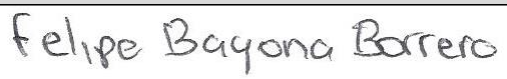
restricción alguna, puesto que de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación de los derechos patrimoniales derivados del régimen del Derecho de Autor.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, "Los derechos morales sobre el trabajo son propiedad de los autores", los cuales son irrenunciables, imprescriptibles, inembargables e inalienables. En consecuencia, la Pontificia Universidad Javeriana está en la obligación de RESPETARLOS Y HACERLOS RESPETAR, para lo cual tomará las medidas correspondientes para garantizar su observancia.

NOTA: Información Confidencial:

Esta Tesis o Trabajo de Grado contiene información privilegiada, estratégica, secreta, confidencial y demás similar, o hace parte de una investigación que se adelanta y cuyos resultados finales no se han publicado. Si [ ] No [X]

En caso afirmativo expresamente indicaré (indicaremos), en carta adjunta, tal situación con el fin de que se mantenga la restricción de acceso.

NOMBRE COMPLETO	No. del documento de identidad	FIRMA
Felipe Bayona Borrero	1020756851	

FACULTAD: Ingeniería

PROGRAMA ACADÉMICO: Ingeniería de sistemas

BIBLIOTECA ALFONSO BORRERO CABAL, S.J.
DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

FORMULARIO

TÍTULO COMPLETO DE LA TESIS DOCTORAL O TRABAJO DE GRADO			
Guía Metodológica para la Administración de la Seguridad Física de la Información en Pymes			
SUBTÍTULO, SI LO TIENE			
AUTOR O AUTORES			
Apellidos Completos	**Nombres Completos**		
Bayona Borrero	Felipe		
DIRECTOR (ES) TESIS O DEL TRABAJO DE GRADO			
Apellidos Completos	**Nombres Completos**		
González Díaz	Joshsua James		
FACULTAD			
Ingeniería			
PROGRAMA ACADÉMICO			
Tipo de programa (seleccione con "x")			
Pregrado	Especialización	Maestría	Doctorado
X			
Nombre del programa académico			
Ingeniería de Sistemas			
Nombres y apellidos del director del programa académico			

Germán Alberto Chavarro Flórez						
TRABAJO PARA OPTAR AL TÍTULO DE:						
Ingeniero de Sistemas						
PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial)*:						

CIUDAD	**AÑO DE PRESENTACIÓN DE LA TESIS O DEL TRABAJO DE GRADO**	**NÚMERO DE PÁGINAS**
Bogotá DC	**2013**	**138**

TIPO DE ILUSTRACIONES (seleccione con "x")

Dibujos	Pinturas	Tablas, gráficos y diagramas	Planos	Mapas	Fotografías	Partituras
		X				

SOFTWARE REQUERIDO O ESPECIALIZADO PARA LA LECTURA DEL DOCUMENTO

Nota: En caso de que el software (programa especializado requerido) no se encuentre licenciado por la Universidad a través de la Biblioteca (previa consulta al estudiante), el texto de la Tesis o Trabajo de Grado quedará solamente en formato PDF.

MATERIAL ACOMPAÑANTE

TIPO	**DURACIÓN (minutos)**	**CANTIDAD**	**FORMATO**		
			CD	DVD	Otro ¿Cuál?
Vídeo					
Audio					

Multimedia					
Producción electrónica					
Otro Cuál?					

DESCRIPTORES O PALABRAS CLAVE EN ESPAÑOL E INGLÉS

Son los términos que definen los temas que identifican el contenido. (*En caso de duda para designar estos descriptores, se recomienda consultar con la Sección de Desarrollo de Colecciones de la Biblioteca* Alfonso Borrero Cabal S.J *en el correo biblioteca@javeriana.edu.co, donde se les orientará).*

ESPAÑOL	INGLÉS
Guía Metodológica	**Methodological Guide**
Seguridad Física	**Physical Security**
Seguridad de la Información	**Information Security**
Administración de riesgos	**Risck Management**

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS

(Máximo 250 palabras - 1530 caracteres)

The Methodological Guide for information´s Physical Security Management in SMEs is a tool for risk management on the physical security of the information assets of small and medium enterprises.

Based on the most used and recognized standards, The Methodological Guide provides step by step instructions to successfully conduct a good information´s physical assurance process in enterprise environments seeking to improve their security through a careful and effective risk analysis.

La Guía Metodológica para la Administración de la Seguridad Física de la Información en Pymes es una herramienta para la gestión de riesgos sobre la seguridad física de los activos de información de las pequeñas y medianas empresas.

Basada en los más usados y reconocidos estándares, la Guía Metodológica brinda un instructivo paso a paso para conducir exitosamente un buen proceso de aseguramiento físico de la información en ambientes empresariales que desean mejorar su seguridad por medio de un cuidadoso y efectivo análisis de riesgos.

GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

CIS1310SD02

FELIPE BAYONA BORRERO

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C
2013

GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

CIS1310SD02

AUTOR
FELIPE BAYONA BORRERO

HTTP://PEGASUS.JAVERIANA.EDU.CO/~CIS1310SD02

DIRECTOR
ING. JOSHSUA JAMES GONZALEZ DIAZ

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C
2013

GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

Rector Magnífico

Padre Joaquín Emilio Sánchez García S.J.

Decano Académico Facultad de Ingeniería

Ingeniero Jorge Luís Sánchez Téllez

Decano del Medio Universitario Facultad de Ingeniería

Padre Sergio Bernal Restrepo S.J.

Director de la Carrera Ingeniería de Sistemas

Ingeniero German Alberto Chavarro Flórez

Director departamento Ingeniería de Sistemas

Ingeniero Rafael Andrés González Rivera

Artículo 23 de la Resolución No. 1 de Junio de 1946

"La Universidad no se hace responsable de los conceptos emitidos por sus alumnos en sus proyectos de grado. Sólo velará porque no se publique nada contrario al dogma y la moral católica y porque no contengan ataques o polémicas puramente personales. Antes bien, que se vean en ellos el anhelo de buscar la verdad y la Justicia."

Agradecimientos

Quiero extender incontables agradecimientos invocando primero el nombre de Dios, dador de vida y fuente inagotable de sabiduría, a todas las personas que me han acompañado en este proceso académico y de vida:

A mis padres Martha Lucía y Eduardo gracias por el incondicionado apoyo y soporte. Son ustedes la mejor guía de honestidad, rectitud y modelo de familia.
A mis amigos, compañeros incansables y buen consejo, gracias por el cariño y por haberme permitido transitar este camino junto a ustedes.

Igualmente a todos mis profesores y a la comunidad javeriana gracias por su admirable vocación y servicio, este camino sería árido sin su constante enseñanza integral y promoción de valores.
A todos mi más sólido agradecimiento y cariño.

Felipe Bayona Borrero

Contenido

Índice de tablas

Índice de gráficas

Abstract

The Methodological Guide for information´s Physical Security Management in SMEs is a tool for risk management on the physical security of the information assets of small and medium enterprises.
Based on the most used and recognized standards, The Methodological Guide provides step by step instructions to successfully conduct a good information´s physical assurance process in enterprise environments seeking to improve their security through a careful and effective risk analysis.

Resumen

La Guía Metodológica para la Administración de la Seguridad Física de la Información en Pymes es una herramienta para la gestión de riesgos sobre la seguridad física de los activos de información de las pequeñas y medianas empresas.
Basada en los más usados y reconocidos estándares, la Guía Metodológica brinda un instructivo paso a paso para conducir exitosamente un buen proceso de aseguramiento físico de la información en ambientes empresariales que desean mejorar su seguridad por medio de un cuidadoso y efectivo análisis de riesgos.

Resumen ejecutivo

La conciencia empresarial entiende cada día más que su más importante activo es su información. Su información representa conocimiento, estrategias, habilidades, posibilidades, oportunidades, ideas, negocio, en conclusión: éxito y rentabilidad.
De aquí que muchos de sus esfuerzos empresariales pueden no tener la fuerza o el impacto esperado si su información corre peligro o es conocida por quien no debiera. La seguridad de la información es una necesidad, ya no un lujo.

La Guía Metodológica para la Administración de la Seguridad Física de la Información en Pymes, es una herramienta que conduce paso a paso a las organizaciones para que realicen un análisis de los riesgos que se ciernen sobre sus activos de información, quienes podrían tratar de materializarlos y cuál sería el impacto que sufriría su organización ante un evento adverso. Con esa información la Guía Metodológica le ayuda a establecer los controles y estrategias para reducir al mayor nivel sus riesgos en seguridad física, brindándole a la organización un espacio más seguro para desarrollar su negocio.

Por medio de cuatro fases la Guía conduce a las organizaciones en primera instancia a conocerse bien a sí mismas, reconocer qué tienen y qué les falta en materia de seguridad. Luego las apoya en un análisis minucioso para determinar los riesgos que puedan ejecutarse por una falla en la seguridad física, para así poder después plantear los escenarios de control apropiados y a la medida para mitigar o ayudar a tratar estos riesgos siempre en pro de la misión institucional. Con este proceso ya finalizado la Guía Metodológica enseña a las organizaciones la importancia del aprendizaje de sus esfuerzos en mejorar su seguridad y en seguir manteniéndose siempre al día y a la vanguardia de los avances de la tecnología y también los del crimen.

Para desarrollar esta Guía Metodológica se hizo una juiciosa investigación sobre los más aplicados y reconocidos estándares a nivel mundial para la gestión de riesgos y la más juiciosa bibliografía sobre seguridad física de la información, con el fin de sintetizar un producto nuevo y propositivo que sirva a las organizaciones.

Luego de todo el desarrollo de la Guía Metodológica, se la lanzó al mundo empresarial para ponerla a prueba y medir sus capacidades., obteniendo excelentes resultados y la aceptación de una organización que reconoce su utilidad y potencial

1. INTRODUCCIÓN

A través de los años, la humanidad se ha visto enfrentada a las diferentes revoluciones que han proporcionado un desarrollo en muchos aspectos, como lo son el social, económico, intelectual, etc. La revolución que hoy enfrentamos es aquella que se conoce como *La revolución de la Información"*, donde se llega a proponer hasta en marcos legales jurídicos, que la información se convierte en uno de los activos más valiosos en nuestra era, tanto así que llega a considerarse un bien jurídico tutelable. [1]

Para dicho activo, sin importar el estado en el que se encuentre (Digital, Documental, Físico, Conocimiento), su proceso de aseguramiento no llega a ser tan sencillo teniendo en cuenta que en nuestro mundo, donde la tecnología avanza a pasos agigantados, constantes y frecuentes, siempre en busca de mejorar la productividad e impulsar las industrias, no se quedan atrás las estrategias y motivaciones para buscar los puntos débiles de estos avances y explotarlos para intereses malintencionados.

Cada nuevo día la información cobra más relevancia como conocimiento y propiedad que genera y sustenta valor en los negocios, y sobre esta base los esfuerzos de las organizaciones por asegurarla de manera adecuada se vuelve una labor primordial y esencial en la búsqueda de mantener el negocio.

Muchas veces la seguridad física es relegada a un segundo plano por la falsa concepción de que el soporte tecnológico de la información se concentra en sus manifestaciones intangibles informáticas y no tanto en los soportes tangibles. Así muchas organizaciones enfocan la mayoría de sus esfuerzos en seguridad en los últimos avances en defensa contra software malicioso, intrusiones y estabilidad informática dejando de lado las exigencias de seguridad que deben tener los equipos que soportan el funcionamiento de estos sistemas lógicos.

Por tal motivo se pensó en la iniciativa de que la guía metodológica muestre y ofrezca a las organizaciones una visión completa desde su análisis hasta su implementación de seguridad física de sus activos de información y hagan una correcta administración de los riesgos asociados a su entorno y funcionamiento físicos como un factor decisivo en su estudio integral de la seguridad en pro de un óptimo desarrollo del negocio y su misión.

1.1 Visión global

Se desarrolló una guía metodológica para la administración de riesgos que implican a la seguridad física de los activos de información, tras el estudio de las metodologías y procedimientos actualmente vigentes y poniéndola a prueba en una organización real del sector financiero colombiano.

1.2 Objetivos y Pregunta de investigación

1.2.1 Formulación

La presente investigación trató de dar respuesta a la pregunta: ¿Cuáles son las falencias empresariales a la hora de asegurar físicamente su información y qué herramientas existen y necesitan para poder lograr o mejorar dicha seguridad?

Para responder a la anterior pregunta primero se realizó una revisión y síntesis de temas como: Los principales riesgos en materia de seguridad física que presentan las organizaciones, las estrategias y metodologías más usadas y las que arrojan mejores resultados en la práctica, los más novedosos ataques en materia de seguridad que atenten contra la integridad, confidencialidad y disponibilidad de los activos de información. En síntesis es una mirada al estado del arte, al mundo empresarial de hoy y a los riesgos e incidentes que día a día se presentan, ocurren o se superan en el desarrollo de la actividad empresarial.

1.2.2 Objetivo general

El objetivo principal de esta investigación fue diseñar una guía metodológica para la administración de la seguridad física necesaria para el aseguramiento de la información en Pymes del sector financiero y evaluar dicha guía en un caso de estudio específico.

1.2.3 Objetivos específicos

- ✓ Realizar un levantamiento de información sobre metodologías o estándares utilizados para el análisis de riesgos de IT
- ✓ Documentar las principales amenazas y escenarios de riesgo que tiene la información que se conocen en el ámbito de seguridad física, realizando además una caracterización sobre aseguramiento de información tanto en modelos lógicos como físicos.

- ✓ Elaborar las plantillas para el desarrollo de los procesos de análisis de riesgos de la información y clasificación de la información.
- ✓ Diseñar una guía metodológica para la administración de la seguridad Física de la información junto a un modelo de administración de la misma.
- ✓ Evaluar la guía metodológica en un caso de estudio, realizando una comparación entre el alcance propuesto por la guía y las necesidades establecidas en el caso.

1.3 Importancia de la investigación

La búsqueda de la optimización en seguridad se ha enfocado en las últimas décadas con especial énfasis en la seguridad lógica o ciberseguridad, dejando atrás puesta sobre un segundo plano a la seguridad física. Las razones de su importancia y el interés en invertir esfuerzo y dinero en ella se basa en la errónea idea de que los incidentes físicos son menos ocurrentes y más manejables.
Pero serán insuficientes los esfuerzos por evitar intrusiones a los sistemas, códigos maliciosos, interceptación y robo de información si el sistema físico es fácilmente accesible por personas que tengan la intención, e incluso los permisos y accesos necesarios para extraer información o sabotear equipos, como bien podría ser el caso de es empleados o empleados descontentos; hasta llegar incluso a enemigos y saboteadores industriales, ladrones, espías corporativos, vándalos o incluso terroristas.

La seguridad física se basa en el aseguramiento para equipo de TI, redes y activos de telecomunicación. Y su importancia en muchos factores se basa en un aspecto económico. Primero, los equipos son costosos de adquirir, de instalar e integrarse con la infraestructura de la organización. Segundo, las operaciones de la organización son dependientes de su infraestructura lo que implica que interrupciones de la operación se tornan rápidamente en costos innecesarios e incluso pérdidas potenciales de ingresos. Tercero, las leyes nacionales respecto al manejo y cuidado de datos e información propietaria almacenados en sistemas de cómputo exigen su protección y en caso de ésta verse comprometida podrían acarrearse litigios.
Así, aunque la relación entre seguridad lógica y seguridad física es estrecha, protegerse solo contra código malicioso o incidentes de hacking resulta insuficiente cuando, por ejemplo, un individuo no autorizado gana acceso a una oficina con equipos conectados a una red y obtiene allí acceso igual o mayor al sistema de lo que podría obtener un hacker, con lo que habrá superado ya muchos obstáculos lógicos de seguridad.
Más adelante se profundizará en más puntos sobre la importancia de la seguridad física, sus obstáculos y formas de optimizarla.

1.4 Alcance y limitaciones:

Alcance: El actual proyecto estuvo definido por la elaboración de la guía metodológica y su validación en un ambiente real empresarial.

Limitaciones: De acuerdo a las limitaciones en el tiempo de desarrollo de todo el trabajo de grado, el proyecto centra sus esfuerzos en el desarrollo completo de la guía metodológica y de una aplicación concreta en una empresa donde puedan explorarse los procedimientos clave de la guía.

1.5 Impacto esperado

Conociendo las guías y procedimientos que se conocen y utilizan actualmente en la industria de la seguridad de la información y la gran variedad de herramientas disponibles para la evaluación de riesgos, pero así mismo la fragmentación de estas y la carencia de unos procedimientos específicos para la administración de riesgos sobre la seguridad física a activos de información, el presente proyecto busca proponer una herramienta nueva que resulte en un producto útil, centralizado y específico para las organizaciones que deseen hacer una evaluación de seguridad de la información y consideren dentro de ese proceso su aseguramiento físico como clave para la continuidad y los intereses de su negocio.

2. ANÁLISIS PRELIMINAR

2.1 Introducción

Desarrollar un proyecto de administración de riesgos y seguridad puede darse para cualquier organización en cualquier momento. Ya sea una empresa nueva o que nunca he generado un plan para el manejo de su seguridad y el control de sus riesgos y ve necesario desarrollarlo, o para otra con más experiencia en el mercado y en la administración de riesgos que sabe de la importancia de mantener su esquema y políticas de seguridad actualizadas y vigentes. En cualquiera de los casos la necesidad siempre está basada en la urgencia por optimizar los mecanismos de protección de las actividades, activos, y dinero que genera la compañía, cuyo objetivo principal siempre es alcanzar su misión de la mejor manera siempre dentro de un marco rentable.

Otro posible caso, que es justamente el que esta guía pretende minimizar, es la necesidad de protegerse a futuro o mitigar una vulnerabilidad que está siendo explotada en el momento cuando un riesgo se materializó. Son contados los casos en los cuales, tras presentarse un acontecimiento adverso, el impacto sea nulo para la compañía. Toda explotación de una vulnerabilidad conlleva un impacto negativo y las medidas deben tomarse lo antes posible, no ya para evitar que el riesgo se materialice, sino para frenar cuanto antes su efecto y estar preparado para una nueva ocasión, y que en ella no se tome a la empresa por sorpresa.

La buena elaboración de políticas de seguridad y procedimiento para encarar los riesgos, las amenazas y su impacto son cruciales para cualquier negocio que desee crecer y mantenerse siempre vigente y resguardado, sin necesidad de tener que aprender de las malas experiencias, sino consciente en todo momento de sus riesgos y posibilidades de forma que las maneje de manera óptima y maximice su operación manteniendo las contrariedades al mínimo.

2.2 La gestión de riesgos

El rol de la gestión de riesgos en la organización es vital en cuanto ayuda a sus directivos en qué grado están como organización expuestos a diferentes riesgos y cuáles deben ser los controles, basados en decisiones estratégicas, que se deben tomar para la mitigación de dichos riesgos.
El NIST 800-30 Risk Management Guide for Information Security Systems [2] define la gestión de riesgos como el proceso que permite a los administradores de sistemas de información balancear el costo operacional y económico de tomar medidas de protección, y aumentar la

ganancia en las capacidades de la misión protegiendo los sistemas e información que la soportan. Del mismo modo define el riesgo en función de la probabilidad de que una amenaza se materialice debido a una vulnerabilidad existente, y de allí surge un impacto que afecta directamente a los proyectos y actividades de negocio.

De este modo se puede ver que la gestión de riesgos hace parte del todo integral de la organización como un proceso sistemático de análisis, valoración y respuesta a los riesgos que se presentan en el desarrollo de sus actividades económicas, a fin de hacerlo aceptable para obtener un resultado optimizado, maximizando la probabilidad de éxito y minimizando la posibilidad e impacto de sucesos adversos.

2.3 Vista preliminar al ciclo de vida de la gestión de riesgos

En general los proyectos emprendidos por una empresa están diseñados sobre un objetivo claro y específico. Todo el esquema de trabajo que se defina va siempre encaminado a una producción óptima y eficiente de sus productos o una buena prestación de sus servicios de modo que se aseguren, entre otros aspectos, la rentabilidad del negocio y todos los factores relacionados que lo apoyen tales como la credibilidad, la puntualidad, la experiencia, la confiabilidad, etc.

Dentro de todo éste proceso de negocio se presentan a diario situaciones que interfieren o dificultan el proceso, y algunas de estas dificultades pueden lesionar o impactar altamente a la organización y su negocio.

De este modo, una necesidad vital en las organizaciones modernas es la de desarrollar, paralelo a sus actividades de negocio, una gestión de todos los posibles riesgos a los que puedan verse sometidos, entendiendo que los esfuerzos que se impriman en este trabajo son determinantes en el buen o mal desarrollo de sus actividades, y que una actitud concienzuda o despreocupada respecto a su gestión de riesgos puede catapultar a la organización al crecimiento y desarrollo o al desprestigio y el fracaso.

Frente al ciclo de vida que tenga esta gestión, es importante señalar que es un proceso iterativo, constante y vivo durante toda la vida de la organización. Un buen conocimiento propio de quien soy cómo organización, con qué cuento, cuánto vale lo que tengo y cómo priorizo esos valores, qué vulnerabilidades y debilidades tengo, y qué controles tomo para reducir el riesgo que estas vulnerabilidades me presentan debe ser un trabajo constante, regular, periódico y muy

incluyente de todo el personal de la organización para que la gestión de los riesgos y más propiamente dicha la seguridad que dicha gestión supone, sea un trabajo mancomunado con un direccionamiento bien definido y al cual todos en la organización se encaminen.

3. DESARROLLO DEL TRABAJO

Para el desarrollo y cumplimiento cabal de los objetivos propuestos para el trabajo de grado, dicho desarrollo se realizó sobre cuatro fases o etapas principales que se siguieron de manera secuencial y cronológica hasta obtener como resultado el cumplimiento de todos los objetivos.

3.1 Fase I: Investigación y levantamiento de la información

3.1.1 Introducción

En esta primera fase del desarrollo del trabajo de grado se hizo un levantamiento juicioso del material disponible en la industria para la gestión de riesgos de la información con el fin de cumplir el primer objetivo específico, obteniendo una base teórica, confiable y ampliamente utilizada para el desarrollo de la Guía metodológica, objetivo principal del presente trabajo de grado.

3.1.2 Estudio base de la investigación

Ya son largos los años y múltiples los esfuerzos que se han ido acumulando en la industria informática para mitigar cada vez más los también constantes ataques y violaciones de seguridad que avanzan a la par con la tecnología y el ingenio. Bajo la premisa de que no existen sistemas totalmente seguros, los esfuerzos se han enfocado en desarrollar cada vez más y mejores tecnologías y herramientas para la mitigación de riesgos, amenazas y problemas de seguridad que se presenten, y si bien no son pocas, el camino nunca acabará y toda nueva propuesta o enfoque valdrá ser tenida en cuenta.

El trabajo de grado se desarrolló con la intensión de proporcionar una herramienta guía en las empresas dirigida por el área de tecnologías de información para el adecuado aseguramiento físico y mitigación de riesgos sobre los activos de información siguiendo los lineamientos base que internacionalmente se encuentran vigentes para tal fin.

Para el manejo de riesgos se tomaron como base diferentes textos ampliamente conocidos y difundidos para la gestión de riesgos de la información. Por un lado está *The Orange Book*, [3] que al día de hoy es una guía general para pensar y desarrollar estrategias y procedimientos de análisis y gestión de riesgos. Así mismo se tomaron como referencia la Guía para el Manejo de Riesgos de los Sistemas de Tecnologías de Información NIST 800-30 [2] del Instituto Nacional

de Estándares y Tecnología, y la Metodología de Análisis y Gestión de riesgos de los sistemas de Información MAGERIT 3.0 [4] como estándares populares que ofrecen herramientas actuales y precisas para la administración de riesgos. Adicionalmente se empleó una muy variada bibliografía sobre seguridad física para empresas y sistemas de TI con el fin de contar con una base sólida y respaldada que dé al trabajo de grado todo el respaldo teórico y el fundamento para ser un excelente producto.

Este trabajo de grado profundizó en procedimientos específicos para el análisis y gestión de riesgos físicos sobre los activos de información de las empresas, piezas clave de todo proyecto y negocio.

Sobre esta base se hizo una investigación sobre el momento actual en ésta área y sus principales buenas prácticas y procedimientos, de donde salió una síntesis para desarrollar una guía metodológica que permita a las empresas diseñar a la medida sus propias políticas y prácticas para el aseguramiento físico de activos de información dirigidos por el área de TI. Finalmente la funcionalidad de ésta guía fue probada mediante un caso de estudio, que demostró los beneficios que trae consigo el buen manejo de riesgos.

3.2 Fase II: Análisis de la información y fuentes de investigación

3.2.1 Introducción

En esta segunda fase, tras haber escogido el material necesario para el desarrollo y fundamento del trabajo de grado, se inició un estudio juicioso de estos textos, sus recomendaciones y esquemas, y se realizó una documentación de ellos. Adicionalmente se hizo un análisis del contexto de seguridad física en la industria colombiana y las normas que rigen a estas empresas respecto a su información y manejo de esta.

3.2.2 Colombia y la seguridad de la información

De los intereses que cobran cada día mayor interés dentro de las organizaciones se encuentran los concernientes a la seguridad de su información sobre la base de que es precisamente ésta el más importante activo para el desarrollo del negocio. De las últimas encuestas realizadas sobre cómo van las empresas colombianas en este campo se observa -reconociendo su avance- una labor aun incompleta al alcanzar los estándares y estadísticas internacionales sobre seguridad.

Según la encuesta "Seguridad Informática en Colombia. Tendencias 2011 – 2012" realizada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) [5] El nivel de participación en la encuesta del sector financiero subió del 10% en 2008 para encontrar su máximo en 2010 con un 15,42%, lo que demuestra que la preocupación por asuntos relacionados con la seguridad de la información cobra cada vez mayor protagonismo en las organizaciones colombiana en su afán de hacer frente a los cada vez más avanzados métodos y modelos de inseguridad, para marchar al paso de los estándares y reglamentos internacionales.

Resulta todavía extenso el trabajo pues Colombia todavía no alcanza una mayoría en el porcentaje de empresas y sectores que se preocupan por la seguridad de su información. Según la misma encuesta –al año 2011– tan solo el 49,3% de los encuestados cuenta con políticas formales, escritas, documentadas e informadas a todo su personal; otro 34,2% dice estarlas desarrollando y un 16,5% asegura no tener políticas de seguridad definidas. Se ha avanzado pero lo recomendable sería un cubrimiento total de inclusión de políticas de seguridad en las organizaciones colombianas.

Al año 2011, 13,82% de los encuestados reconoce haber sufrido ataques de ingeniería social a su personal, 7,24% suplantación de identidad, 3,29% espionaje, 17,11% robo de hardware, y 10,53 robo o fuga de información, lo que muestra un remanente sustancial de brechas de seguridad a combatir como un reto por un mejor aseguramiento de la información.

3.2.3 Metodología Orange Book

El Orange Book [3] es una guía, diseñada por el Her Magesty´s Treasury (El tesoro de Su Majestad) departamento de gobierno del reino unido encargado de las políticas económicas y fiscales, que establece el concepto de administración de riesgos y provee una introducción básica a sus conceptos, su desarrollo y la implementación de procesos de administración de riesgos para las organizaciones.

El Orange Book define un proceso no lineal para la administración de riesgos. Define este proceso como el balance de elementos entretejidos que interactúan entre ellos. Anota además que los riesgos específicos no pueden ser direccionados de forma aislada del resto porque el manejo de uno puede impactar al otro.
En este proceso iterativo define las siguientes etapas:

- ✓ Identificación de riesgos

- ✓ Clasificación de riesgos
- ✓ Evaluación de riesgos
- ✓ Tolerancia al riesgo
- ✓ Direccionamiento de riesgos
- ✓ Revisión y soporte de riesgos

Éstas a su vez atravesadas en todo momento por las siguientes actividades:

- Comunicación y aprehensión
- Evaluación del ambiente de riesgo y contexto

Ilustración 1: Modelo de manejo de riesgos – Orange Book

3.2.3.1 Identificación de riesgos:

Es el primer paso en la definición del perfil de riesgos de la organización y su documentación es crítica para el buen manejo de los riesgos.
Los riesgos deben estar siempre relacionados con los objetivos del plan, ya sean personales, del proyecto o de la compañía

La identificación puede darse en dos fases:

- **Identificación inicial de riesgos:** Para una organización que no ha hecho su análisis de riesgos, o para una organización nueva o un nuevo proyecto.
- **Identificación continuada de riesgos:** Para identificar los riesgos no observados anteriormente, los cambios vistos en los riesgos, o lo nuevos riesgos que antes no existían.

El Orange Book recomienda adoptar una buena herramienta para la identificación de riesgos. Por ejemplo:

- **La puesta en marcha de una visión general de los riesgos:** Se establece un equipo designado para considerar todas las actividades y operaciones en relación con sus objetivos, e identificar sus riesgos asociados. El equipo debe trabajar conduciendo una serie de entrevistas con el personal clave en todos los niveles de la organización para lograr un perfil de riesgos.
- **Autoevaluación de los riesgos:** Aquí se invita a todos los niveles de la organización a evaluar sus actividades e identificar los riesgos asociados a ellas. Esto puede ser por medio de un marco de trabajo, cuestionarios o la guía de algún especialista.

3.2.3.2 Clasificación de riesgos

Propone la siguiente clasificación:

- **Externos:** Derivados del ambiente externo a la compañía, que no tiene control total sobre ellos, pero puede tomar acciones para mitigarlos. Pueden ser de tipo:
    - Político
    - Económico
    - Sociocultural

  - Tecnológico
  - Legislativo o regulatorio
  - Ambiental

- **Operacionales:** Relacionados con la operación de la compañía. Pueden ser de Entrega, de Capacidad y de Rendimiento en administración de riesgos:
  - Entrega:
    - Falla en el servicio o el producto - Entrega del proyecto
  - Capacidad:
    - Recursos (Financieros, de información y físicos)
    - De relaciones (con empleados, clientes y proveedores) - Operaciones – Reputación
  - Rendimiento en administración de riesgos:
    - "Governance"
    - Escaneo y búsqueda
    - Resistencia
    - Seguridad

- **Cambio:** Riesgos creados por decisiones en buscas de ir más alá de la capacidad actual.
  - Cambio de programas
  - Nuevas políticas
  - Nuevos proyectos

3.2.3.3 Evaluación de riesgos

Tres principios básicos:

- Asegurarse de que hay un proceso claro y estructurado donde probabilidad e impacto estás definidos para cada riesgo.
- Documentar la evaluación de riesgos de manera que facilite su monitoreo y prioridades.
- Ser claro en la diferencia de riesgo inherente y riesgo residual.

Algunos riesgos permiten un diagnóstico numérico, otros por el contrario requieren de una visión más subjetiva.

La valoración puede hacerse probabilidad VS. impacto, con una clasificación: bajo, medio o alto que suele ser suficiente. Esto genera una matriz de 3x3 sobre la que se pueden definir unos límites de tolerancia.
También suela hacerse con una matriz 5x5 con el impacto clasificado en: Insignificante, menor, moderado, alto y catastrófico; y la probabilidad en: Rara, improbable, posible, probable y casi segura.

Es difícil de calcular el nivel de tolerancia al riesgo, pero para el caso de uno concreto se puede evaluar en términos de tolerancia de impacto y tolerancia de frecuencia. En términos de frecuencia es mejor enfocarse en el riesgo residual, que por supuesto tras encontrado, debe ser revalorado.

3.2.3.4 Tolerancia al riesgo

Debe considerarse tanto para amenazas como para oportunidades.
En el caso de las amenazas el concepto abarca el nivel de exposición considerado tolerable y justificable. Para las oportunidades abarca cuánto se es capaz de poner en riesgo en comparación a los beneficios de la oportunidad.
En los casos en que los riesgos no pueden ser mitigados se debe crear un plan de contingencia.

También puede ser analizado como:

- Tolerancia al riesgo comparada: Es el total acumulado de riesgo que se juzga apropiado para una organización tolerar según sus directivas. Los directivos deben juzgar el rango tolerable de exposición y definir límites para el riesgo inaceptable.
- Tolerancia al riesgo delegada: se trata de diferentes niveles de tolerancia de acuerdo a los diferentes niveles de la empresa. El efecto de esto es que lo que es considerado un alto nivel de riesgo en cierto nivel, será de menos nivel de riesgo en otro nivel más alto de administración.
- Tolerancia al riesgo de proyectos.: Los proyectos que se dan día a día en la organización pueden necesitar otro tipo de tolerancia de acuerdo a su tipo: Especulativos(a mayor riesgo mayor ganancia), estándar, y de misión crítica (el éxito debe estar asegurado)

3.2.3.5 Direccionamiento de riesgos

El objetivo es volver la incerteza beneficio de la organización, limitando las amenazas y tomando ventaja de las oportunidades. Esto se conoce como *Control Interno.* Hay 5 claves para el direccionamiento:

- Tolerar: La exposición es tolerable sin que se tome ninguna acción.
- Tratar: Mientras las actividades de la organización siguen desarrollándose, se toman acciones para llevar los riesgos a niveles tolerables.
- Transferir: Puede hacerse desde tomar un seguro convencional, o pagando a un tercero para que tome el riesgo. Esta opción es particularmente válida para riesgos financieros o de activos.
- Terminar: Algunos riesgos solo son tratables o contenibles en niveles aceptables terminando la actividad.
- Tomar la oportunidad: No es alternativa a las anteriores, incluso vale la pena tomarla en cuenta cuando se asume la tolerancia, la transferencia o el tratamiento. Hay 2 aspectos: el primero es cuando mientras se mitigan riesgos una oportunidad positiva aparece; la segunda es si aparecen circunstancias mientras no aparecen riesgos u oportunidades positivas.

La opción de tratar puede, a su vez, ser vista desde 4 formas de control:

- Controles Preventivos: Diseñados para limitar la posibilidad de un resultado no deseado
- Controles Correctivos: Diseñados para corregir resultados indeseables ya acontecidos. Dan alguna ruta para la recuperación de pérdidas o daños.
- Controles Correctivos: Diseñado para asegurar que algún resultado es alcanzado. Particularmente importantes cuando es crítico que un resultado no deseado se dé, como en los campos de la salud y la seguridad.
- Controles de Detección: Diseñados para identificar un resultado indeseado luego de que ha ocurrido. Por esta naturaleza son apropiados sólo cuando son aceptables el daño o la pérdida incurridos.

3.2.3.6 Revisión y reporte de riesgos

La administración de riesgos debe ser revisada y reportada:

- Para monitorear si el perfil de riesgos está cambiando o no.

- Para ganar certeza de que el manejo de riesgos es efectivo y cuándo una nueva acción debe ser tomada.

Los procesos deben ser documentados en orden para ver si los riesgos aún existen, si nuevos riesgos han aparecido, si la posibilidad y el impacto han cambiado, para reportar cambios significativos que requieran reajustar prioridades, y poder valorar la efectividad de los controles. Este proceso debe:

- Asegurarse que todos los aspectos de la administración de riesgos son revisados al menos una vez al año.
- Asegurarse que los riesgos como tal son revisados con frecuencia.
- Prever para alertar a la gestión de nivel adecuado de los nuevos riesgos o los cambios en los ya identificados para que puedan ser bien direccionados.

La auditoría interna provee una importante independencia objetiva para la evaluación acerca de lo adecuado de las políticas y controles de administración de riesgos.

3.2.3.7 Comunicación y aprehensión

Se ejecuta durante todo el proceso de administración de riesgos.
La identificación de nuevos riesgos o cambios en los existentes depende de la comunicación., en particular de mantener una buena red de comunicación con contactos relevantes y fuentes de información.

Es importante para asegurarse de que todos los empleados entiendan cual es la estrategia de manejo de riesgos de la empresa, cuales riesgos son prioritarios, y cómo sus responsabilidades particulares dentro de la empresa encajan en ese marco.

Es también importante que todos los niveles de administración, busquen activamente y reciban asistencia apropiada y regular acerca del manejo de riesgos.

Es importante comunicarse con los stakeholders acerca de la forma en que la organización está manejando los riesgos, para darles garantía de que la organización se comportará de la manera que ellos esperan, y para manejar sus expectativas de lo que podría ser la organización.

3.2.3.8 Ambiente de riesgo y contexto

Muchos factores participan en el ambiente en que los riesgos deben ser administrados. Estos factores pueden generar riesgos que no pueden ser directamente controlados o limitan las formas en que la organización puede direccionar esos riesgos.
La única respuesta que la organización puede tomar contra estos riesgos es realizar planes de contingencia en caso de que ocurran.

En particular, las leyes y regulaciones pueden tener un efecto en el contexto de los riesgos. Es importante que las organizaciones identifique la forma en que éstas regulaciones les demandan, incluso solicitándoles acciones y restringiéndole otras que las organizaciones se permitirían tomar.

3.2.4 Metodología NIST 800- 30

La Guía para el manejo de riesgos de Sistemas de Tecnologías de Información NIST 800-30 [2] es un estándar que tiene como objetivo ayudar a las organizaciones a llevar un proceso de gestión de riesgos para que aseguren su misión, por un lado mejorando la seguridad de sus sistemas de información encargados de almacenar, procesar o transmitir información del negocio, también dando un insumo para que la administración pueda tomar decisiones inteligentes de negocio basándose en el conocimiento de sus riesgos, y por último asistiendo a la administración a llevar una correcta documentación de este conocimiento de sus sistemas y sus riesgos para producir buenos resultados en su gestión.

El proceso de gestión de riesgos de la NIST 800-30 contempla 9 pasos fundamentales como siguen:

- ✓ Paso 1: Caracterización de los sistemas
- ✓ Paso 2: Identificación de amenazas
- ✓ Paso 3: Identificación de vulnerabilidades
- ✓ Paso 4: Análisis de controles
- ✓ Paso 5: Determinación de la probabilidad
- ✓ Paso 6: Análisis de impacto
- ✓ Paso 7: Determinación de riesgos
- ✓ Paso 8: Recomendaciones de control
- ✓ Paso 9: Documentación de resultados

Ilustración 2: Actividades de gestión de riesgos NIST 800-30

Seguido a esto, la NIST 800-30 propone el modelo de mitigación de riesgos que comprende los siguientes temas:

- ✓ Paso 1: Priorizar acciones
- ✓ Paso 2: Evaluar las opciones de control recomendadas
- ✓ Paso 3: Realizar un análisis de costo – beneficio
- ✓ Paso 4: Seleccionar controles
- ✓ Paso 5: Asignar responsabilidades
- ✓ Paso 6: Desarrollar plan de implementación de salvaguardas
- ✓ Paso 7: Implementar controles seleccionados

Paso 1: Priorizar acciones	•Entradas: Niveles de riesgo del reporte de gestión de riesgos •Salidas: Ranking de acciones de muy a poco importantes
Paso 2: Evaluar las opciones de control recomendadas	•Entradas: Reporte de gestión de riesgos •Salidas: Lista de posibles controles
Paso 3: Realizar un análisis de costo – beneficio	•Salidas: Análisis de costo - beneficio
Paso 4: Seleccionar controles	•Salidas: Controles seleccionados
Paso 5: Asignar responsabilidades	•Salidas: Lista de personas propuestas
Paso 6: Desarrollar plan de implementación de salvaguardas	•Salidas: Plan de implenetación de salvaguardas
Paso 7: Implementar controles seleccionados	•Salidas: Riesgo residual

Ilustración 3: Actividades de mitigación de riesgos NIST 800-30

Sobre estas actividades la NIST 800-30 establece, además de las definiciones y procedimientos comunes en la mayoría de guías de gestión de riesgos, unos pasos concretos y de sencilla implementación para llegar con éxito a una buena gestión de riesgos.

3.2.5 Metodología MAGERIT 3.0

La metodología de análisis y Gestión de Riesgos de sistemas de información MAGERIT, [4] es un documento elaborado por el consejo superior de administración eléctrica de España en respuesta a la cada vez más creciente utilización de sistemas de información tanto en organizaciones privadas como estatales, y la importancia que estos sistemas cobran proporcional al tiempo y mejoramiento.

Magerit resalta como objetivos principales el concienciar a los responsables de las organizaciones de la existencia de riesgos y la necesidad de gestionarlos, además de descubrir y planificar su tratamiento oportuno por medio de un método sistemático.

Magerit nos define seguridad como la capacidad de los sistemas de información de resistir en el mejor grado posible las actuaciones ilícitas o incidentes que comprometan la disponibilidad, la confidencialidad, la integridad o la autenticidad de los datos. Así mismo nos define el riesgo como la estimación del grado de exposición a que una amenaza se materialice causando daños

a la organización (cabe notar que la concepción de riesgo de Magerit es exclusiva sobre el riesgo negativo).

Magerit define su metodología alrededor de 2 grandes fases:

- Análisis de riesgos: Esta primera etapa se basa en conocer a la empresa y saber qué le puede pasar. Aquí se detallan entonces cuales son los activos , se valoran, se detectan sus amenazas, se determina el impacto que tendrían, el riesgo y la selección de salvaguardas

- Gestión de riesgos: Aquí se detalla el proceso de organización de la defensa, que en última intención es lograr que los valores de riesgo e impacto residuales sean aceptables para la organización.

La guía Magerit presenta con un mayor nivel de detalle la elaboración de un proyecto de análisis y gestión de riesgos, y las actividades más puntuales que éste debe abarcar, además de las tareas propias que deben asumir los empleados de acuerdo a su rol dentro del proyecto.

Resaltable de Magerit es que nos ofrece un *Catálogo de Elementos* donde además de las definiciones y procedimientos de gestión de riesgos que otras metodologías ofrecen, brinda una excelente guía para el levantamiento de activos de información, las formas más adecuadas de valorarlos y una muy completa lista de amenazas y salvaguardas que pueden ayudar a las organizaciones a direccionarse mejor en ese proceso de gestión de riesgos.

3.2.6 Una visión sobre la seguridad física

La seguridad física sobre activos de información, tecnología de redes y equipos de comunicaciones ha sido constantemente pasada por alto por muchas organizaciones. Esto se debe en parte al gran número de organizaciones que han adquirido la noción de que en la medida en que la tecnología avanza deben ser mayores los esfuerzos en protegerse en un entorno lógico y no tanto físico. Pero esta idea ha venido cambiando en la medida en que dicho crecimiento tecnológico ha implicado un crecimiento también en equipos para los cuales las estructuras, edificios e instalaciones de las organizaciones no están perfectamente preparados o diseñados.

La importancia de la seguridad física se fundamenta en varias razones, muchas de ellas económicas: Primero, los equipos son costosos de conseguir, instalar e integrar dentro de la infraestructura de las organizaciones. Segundo, las operaciones de las organizaciones, incluidas todas las operaciones informáticas basadas en software, están soportadas por una infraestructura tecnológica. Tercero, en la mayoría de los países dependientes de los computadores y la tecnología tienen leyes que exigen la protección de datos e información almacenada en equipos de cómputo, por lo cual su compromiso puede potencialmente conllevar a procesos jurídicos.

Aunque suele hacerse especial énfasis en la implementación de seguridad lógica debido al creciente número de incidentes de hacking o amenazas por código malicioso, es importante tener en mente la estrecha relación que existe entre la seguridad lógica y la seguridad física de sistemas IT, siendo la más obvia que si una persona no autorizada gana acceso a una oficina que tiene un computador conectado a la red interna, ésta persona podrá tener igual o mayor acceso a los sistemas de la organización que cualquier hacker externo.
Un acceso no autorizado de estas características puede ser conducido potencialmente a establecer un uso no autorizado de cuentas privadas de usuario, plantar troyanos o programas espía en los sistemas, conseguir acceso a información protegida o robar información propietaria de la organización.

El punto aquí es que no importa cuánto se invierta en seguridad lógica si una persona puede caminar fácilmente hacia el acceso de un sistema que está sumergido en toda clase de protecciones lógicas. Así mismo el robo de equipos portátiles y móviles es un gran riesgo por el acceso que tienen a sistemas internos, lo que presenta una debilidad que debe ser muy bien evaluada, entre otras muchas situaciones que evidencian la estrecha correlación de seguridad física y lógica y el tratamiento igualitario que se les debe prestar. [6]

Caso Stuxnet: Una aproximación a la ciberguerra entre naciones.

Con el desarrollo tecnológico, en el siglo XXI parece abrirse campo paralelamente el campo de la guerra digital o ciberguerra. Ya el gobierno de los Estados unidos ha decretado internacionalmente el ciberespacio como el quinto dominio de la guerra junto a la tierra, el mar, el aire y el espacio. En Colombia ya se ha creado el primer comando Conjunto Cibernético del Ejército Nacional dedicado exclusivamente a labores de ciberdefensa.

El caso del ataque a Irán con el gusano Stuxnet es clara muestra de la estrecha relación que existe entre la seguridad lógica y la seguridad física, y cómo un fallo en alguna de las dos puede hacer colapsar a la otra, causando así daños tanto lógicos como estructurales.
En junio de 2010 los Laboratorios Kaspersky alertaron sobre la existencia de un gusano de 500 kilobytes que había infectado al menos 14 plantas industriales en Irán, siendo una de ella una planta de enriquecimiento de uranio, material fundamental para la obtención de energía nuclear. Según Kaspersky Labs ya hay desarrollados en el mundo programas informáticos capaces de atacar represas de agua, paralizar plantas de energía, bancos e infraestructura que antes se consideraba inmune a ataques informáticos.

El gusano Stuxnet funciona en seis diferentes fases:

1. **Infección:** Stuxnet ingresa al sistema vía USB y procede a infectar todas las máquinas que corran Microsoft Windows utilizando un certificado digital que pareciera venir de una compañía confiable. Puede evadir sistemas de detección automatizados.
2. **Búsqueda:** Stuxnet procede a evaluar cuál máquina infectada corresponde al sistema de control industrial a atacar que opere bajo el software Step7 de Siemens. Estos sistemas son utilizados en Irán para controlar las centrifugadoras utilizadas en el proceso de enriquecimiento del uranio.
3. **Actualización:** Si el sistema infectado no es un objetivo, Stuxnet no hace nada. Caso contrario busca el modo de acceder a internet para actualizarse a sí mismo.
4. **Compromiso:** Stuxnet empieza a comprometer los controladores lógicos del sistema explotando vulnerabilidades de día cero, debilidades del sistema que aún no han sido identificadas por los expertos.
5. **Control:** El gusano empieza labores de espionaje del sistema para entender todo su funcionamiento. Ya con suficiente información recolectada toma control del sistema y empieza a atacar la infraestructura.
6. **Engaño y destrucción:** Mientras ejecuta todos los cambios en los controladores, informa al sistema de monitoreo falsos reportes de buen funcionamiento para asegurarse de que no se tomen medidas hasta que los daños sean irreparables.

En el caso iraní, el virus entró vía USB por medio posiblemente de un incauto ya que obviamente el sistema de control de una planta de enriquecimiento de uranio no está conectado a internet. Una vez adentro invadió todo el sistema y aprendió de él hasta entender los ciclos de centrifugado del material nuclear. Con esta información empezó a variar las velocidades de los ciclos de modo tal que se diera un sobrecalentamiento y un daño de las centrifugadoras. Al

mismo tiempo enviaba informes de funcionamiento normal a los controladores del proceso lo que ocultaba el daño físico real que se estaba causando. [7]

Irán no se ha pronunciado oficialmente sobre los daños causados, pero lo relevante de este caso es analizar, por un lado, el tipo de atacantes, que de acuerdo a las cualidades del software malicioso, su complejidad y objetivos parece imposible que fuera desarrollado por un particular, pareciendo necesitar del apoyo de uno o más estados-nación para su desarrollo. Por otro lado que su actuación, aunque aparentemente virtual, es posible gracias a la explotación de vulnerabilidades en la seguridad física; y sus objetivos van más allá de capturar o alterar la integridad de datos informáticos, llegando a alterar y dañar sistemas SCADA y la infraestructura física que controlan.

El anterior ejemplo como un caso a gran escala de la importancia de la seguridad física y su relación indesligable con la seguridad lógica.

3.2.7 Contexto legislativo colombiano

3.2.7.1 Ley 1273 de 2009

La Ley 1273 de 2009 es una modificación del código penal colombiano por el cual se busca proteger íntegramente a los sistemas que utilizan tecnologías de la información y la comunicación, entre algunas otras disposiciones.
Llamada "de la protección de la información y de los datos", la Ley 1273 adiciona 2 capítulos al código penal colombiano: Uno regulando las disposiciones sobre los atentados contra los 3 principios fundamentales de la seguridad de la información (Integridad, disponibilidad y confidencialidad), y uno segundo sobre los atentados informáticos.

El Capítulo I titulado: *De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas de información*, define las condenas punitivas, tanto carcelarias como económicas, para las siguientes circunstancias fuera de la ley.

- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de comunicación.
- Interceptación ilegal de datos informáticos.
- Daño informático.
- Uso de software malicioso.
- Violación de datos personales.

- Suplantación de sitios web para obtención de datos personales. Aplica también para DNS

El capítulo I define también circunstancias de agravamiento en caso de cometer las conductas:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

El Capítulo II titulado: *De los atentados informáticos y otras infracciones*, define las condenas punitivas, tanto carcelarias como económicas, para delitos que sean cometidos usando un sistema de información o red de comunicaciones.

- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.

La Ley 1273 es promulgada y empieza a regir desde el 5 de enero de 2009 y deroga el artículo 195 del código penal y todas las disposiciones que le son contrarias. [8]

3.3 Fase III: Desarrollo de la guía metodológica y las plantillas de apoyo

3.3.1 Introducción

En esta tercera fase de desarrollo del trabajo de grado dar cumplimiento al objetivo general propuesto por medio del desarrollo de la Guía Metodológica para la Administración de la Seguridad Física de la Información en Pymes, las plantillas que soportan sus procesos, y la aplicación de la misma en una empresa del sector financiero con el fin de probar su

funcionalidad y efectividad como producto para la gestión de riesgos enfocada a la seguridad física de la información.

Esta fase se desarrolló apoyada en toda la información recolectada y seleccionada en las dos fases inmediatamente anteriores, además de toda la información bibliográfica consultada sobre seguridad física, políticas y buenas prácticas en esta área de la seguridad de la información

3.3.2 La guía metodológica y las plantillas

El desarrollo de la Guía Metodológica y sus plantilla de apoyo fue un trabajo paralelo ya que las plantilla son un insumo en cada una de las fases descritas dentro de la metodología. Ya teniendo una base teórica para desarrollar la guía metodológica se inició su redacción, un proceso que tardó alrededor de 7 semanas.

La Guía Metodológica se estructuró sobre 4 fases entorno a un esquema propuesto para la gestión de riesgos.

3.3.2.1 Esquema propuesto para la administración de riesgos

El modelo que propone la Guía Metodológica pretende proporcionar una herramienta para la identificación y gestión de riesgos correspondiente a aspectos de la seguridad física dentro de la compañía. Este consiste en una serie de pasos secuenciales que permitirán al equipo encargado de la evaluación de riesgos y seguridad de IT llevar el proceso de manera más ordenada y eficiente. Es importante también recordar que este proceso no es de realización única, debe por el contrario ser un proceso iterativo, de constante revisión y actualización, y que debe articularse con todas las áreas de la compañía y sus equipos de trabajo.

La fase de análisis de riesgos pretende establecer una lista de riesgos clasificados según su prioridad, determinada por la probabilidad de materialización de un riesgo particular y la magnitud del impacto que genere su ocurrencia. De este modo, una prioridad alta es dada a un riesgo que resulta ser más crítico y por esta misma naturaleza debe ser mitigado con mayor prontitud sin olvidar el costo relacionado con dicha medida. Para determinar el impacto de materialización de un riesgo vale la pena plantearse preguntas del estilo: ¿qué puede, cómo y por qué puede ocurrir? ¿Qué tan malo puede ser y a quienes afectaría?

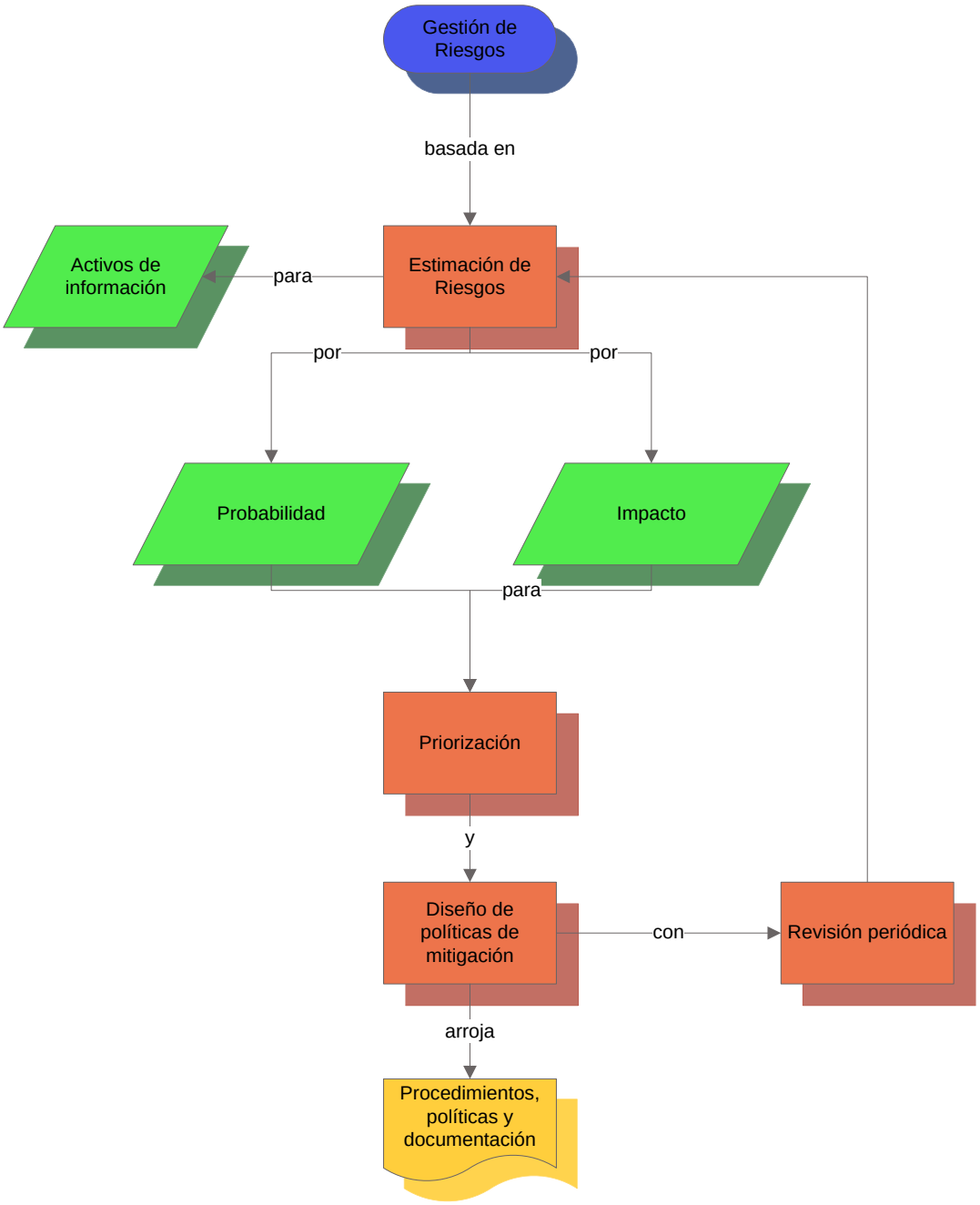
El modelo que se propone ayudará a evaluar y gestionar cualquier riesgo independientemente de su prioridad. Es importante aclarar que la guía no representa una "camisa de fuerza" frente a los procedimientos y definiciones para la administración de riesgos: Cada organización puede adaptar las propuestas de la presente guía de acuerdo a sus particularidades y necesidades.

Una vez identificados, analizados y priorizados los riesgos se procede a establecer los mecanismos de respuesta ante ellos que permitan direccionarlos en la mayor medida posible. Es importante recordar que sólo en contadas ocasiones es posible la mitigación del 100% del riesgo.

Así entonces el proceso se basará, en primera instancia, en un levantamiento de información que permitirá conocer los activos de información de la compañía para luego identificar los posibles riesgos a los que se ven expuestos. Tras esto se elabora un análisis de dichos riesgos de acuerdo a las variables de probabilidad e impacto y por medio de una escala se priorizan los mismos para por último diseñar las tácticas propias de mitigación.

Todo el anterior proceso debe documentarse debidamente en cada etapa para así poder hacer un seguimiento del proceso de administración de riesgos, que por su carácter iterativo debe estar en constante revisión y actualización. Así mismo todos estos resultados deben verse reflejados en el diseño de políticas de seguridad que describan las bases y procedimientos para todos los trabajadores de la compañía que tengan relación con sus activos de información. ¡La seguridad es un trabajo conjunto y mancomunado de esfuerzos de todos en la compañía!

El siguiente gráfico muestra el esquema propuesto para la administración de riesgos:



3.3.2.2 Fases de la guía metodológica

De acuerdo al esquema anterior se definieron 4 fases que estructuraran la columna vertebral de los procesos de la guía metodológica. Esta decisión se tomó en base a la experiencia del Ingeniero González y la estructura esencial que deseábamos construir en la guía para el proceso de administración de riesgos, haciendo una clara separación de las etapas del proceso, su desarrollo a la hora de la implementación y el agrupamiento de tareas acorde a cada etapa del proceso de gestión.

Así entonces se definieron las siguientes 4 fases:

I. Fase I: Caracterización de la organización.
II. Fase II: Gestión de riesgos.
III. Fase III: Desarrollo de controles y Mitigación de riesgos.
IV. Fase IV: Revisión y documentación.

En busca de un factor diferenciador que permitiera a la Guía Metodológica aportar un nuevo enfoque adicional a las metodologías ya existentes (además, claro está, de su enfoque en la seguridad física) se determinó que un eje central de la gestión de riesgos que propusiera la guía debía ser el de llevar a cabo cada uno de sus procedimientos enfocado en el aseguramiento de cada uno de los 7 principios de la seguridad de la información, ya que es usual que las metodologías más comunes se centren solo en las mediciones de la integridad, la confidencialidad y la disponibilidad de la información.

Así entonces, antes de entrar a definir cada fase, se definen los 7 principios de la seguridad de la información que serán eje de atención en cada fase, así:

- **Integridad:** Garantiza la exactitud de la información y que siempre sea completa. Es decir, que la información válida que se registró, o la estructura original o válidamente configurada del activo se mantiene como fue dispuesta por quien está autorizado.

- **Confidencialidad:** Garantiza que la información solamente es accesible a las personas autorizadas para tener acceso. Esto incluye que no sea interceptada, vista, accedida o modificada por usuarios no autorizados.

- **Disponibilidad:** Garantiza que los usuarios puedan tener acceso a la información en el momento requerido. Es decir que los activos de información están disponibles para los usuarios autorizados cada vez que estos los requieran.

- **Autenticación:** Garantiza que quien solicita un acceso es quien dice ser. Es decir que se corrobora que los usuarios que solicitan acceder a activos de información corresponden en la dupla ser-identificación.

- **Autorización:** Garantiza que alguien o algo acceda únicamente a lo que se le es permitido. Es decir que cualquier usuario que cuente con diferentes permisos sobre activos de información sólo pueda acceder a los permitidos por sus privilegios.

- **No repudiación:** Garantiza que quien genera un evento válidamente, no puede retractarse. Esto para llevar un seguimiento de acciones de los usuarios para saber quién hizo qué y que no pueda negarlo u ocultarlo.

- **Observancia:** Garantiza el adecuado funcionamiento de la seguridad. Es decir que las políticas y procedimientos son seguidos según lo especificado y que se cumplen las medidas de seguridad y funcionan los sistemas.

Sobre esta definición empieza el desarrollo de cada una de las 4 fases.

Fase I: Caracterización de la organización:

Esta primera fase pretende hacer una caracterización integral de la organización para conocer cuáles son sus procesos y activos ligados a proteger, cuales deben priorizarse de acuerdo a la criticidad que tenga su rol en la misión y objetivos de la organización, y cuáles son los controles y políticas existentes para la gestión de riesgos y el aseguramiento físico de la organización.

Contenidos dentro de esta primera fase se encuentran dos procedimientos esenciales para la administración de riesgos: Por un lado la identificación de activos de información y por otro las técnicas de levantamiento de la información.

El levantamiento de activos se basa en el Catálogo de Elementos de MAGERIT 3.0 [4] que facilita una guía sobre levantamiento de activos, amenazas y definición de salvaguardas. Sobre este marco teórico se desarrolló la siguiente clasificación de activos:

- Información general
- Información de funcionamiento
- Servicios
- Hardware
- Redes de comunicaciones
- Soportes de información
- Equipos auxiliares

- Instalaciones
- Personal

Junto a las definiciones de estas categorías de activos se desarrollaron las plantillas para su levantamiento y su valoración respectiva sobre los 7 principios de la seguridad de la información.

Sobre las plantillas y el levantamiento de activos y su valoración se decidió que el proceso debía llevarse para cada activo, por lo que el diseño de cada plantilla de clasificación y valoración parte del encabezado de *Nombre del activo* y un *Código* único de identificación. De este modo al hacer el levantamiento de activos se recoge información puntual de cada uno y se valora cada uno sobre los 7 principios para poder así hacer un análisis de riesgo completo para cada uno. Es probable, claro, que muchos activos por el hecho de compartir el mismo ambiente o recursos estén sometidos a las mismas amenazas, por ejemplo, pero sus características propias, sus controles y su criticidad si pueden ser diferentes y por ello requieren un análisis individual.

Frente a la priorización de los activos respecto a los 7 principios de la seguridad de la información se definieron los siguientes criterios:

- ✓ **Integridad:** ¿Qué tanto se perjudicaría la organización con variaciones en la integridad de los activos?
- ✓ **Disponibilidad:** ¿Qué tanto se perjudicaría la organización si sus activos no estuvieran disponibles o parcialmente disponibles?
- ✓ **Confidencialidad: ¿**Qué tanto se perjudicaría la organización si sus activos de información fueran conocidos o utilizados por personas no autorizadas?
- ✓ **Autenticación:** ¿Qué tanto se perjudicaría la organización si el personal con el que cuenta o las personas que la frecuentan no son quienes dicen ser?
- ✓ **Autorización:** ¿Qué tanto se perjudicaría la organización si su personal o personas que la frecuentan obtuvieran accesos más allá de sus capacidades y permisos?
- ✓ **No repudiación:** ¿Qué tanto se perjudicaría la organización si no puede saber quién o quienes hicieron qué con sus activos e información?
- ✓ **Observancia:** ¿Qué tanto se perjudicaría la organización si no aplica controles de seguridad a sus activos?

Con estas preguntas clave la Guía metodológica propone una aproximación inicial al valor de los activos en la empresa

Esta valoración inicial se decidió medirlo en una escala de 1 a 5, o de muy bajo a muy alto, de acuerdo a la evaluación cuantitativa o cualitativa y a su importancia para el negocio y la organización como se muestra a continuación:

Escala Cualitativa	Escala Cuantitativa	Descripción
Muy Bajo	1	Irrelevante para el negocio
bajo	2	Importancia menor o auxiliar para el negocio
Medio	3	Importante para el negocio
Alto	4	Altamente importante para el negocio
Muy Alto	5	De actuación crítica. El negocio depende fuertemente de él.

Tabla 1: Tabla de priorización de activos

Frente a las técnicas de levantamiento de información se propusieron (aunque no se especificaron) además de las plantilla, los cuestionarios, las entrevistas, la revisión de documentación y la utilización de herramientas automatizadas.

Fase II: Gestión de riesgos

Nuevamente, para iniciar la fase se dieron algunas definiciones con el fin de unificar términos a los lectores.

- **Amenaza:** Es el potencial que tiene una fuente de amenazas para disparar accidentalmente o explotar deliberadamente una vulnerabilidad.

- **Fuente de amenaza:** Es una intención y un método dirigidos a la explotación intencional de una vulnerabilidad, o bien una situación y un método que pueden accidentalmente disparar una vulnerabilidad. Vale la pena resaltar que una fuente de amenaza no representa un riesgo en la medida en que no haya una vulnerabilidad qué explotar o disparar.

- **Vulnerabilidad:** Se entiende como una falla o una debilidad en procedimientos de seguridad, diseño, implementación o control sobre sistemas que se puede disparar accidentalmente o ejecutar intencionalmente, generando una brecha de seguridad o en una violación de sus políticas.

Esta fase se definió para el conjunto de todas las acciones que abarcan la gestión del riesgo luego del levantamiento de la información y antes del desarrollo de controles y la mitigación de

los riesgos. Es en síntesis, la fase del descubrimiento del riesgo inherente de los activos de información.

Esta fase abarca entonces todos los procedimientos para identificar las amenazas y sus fuentes, levantar sobre eso las vulnerabilidades que pueden ser explotadas y valorarlas de acuerdo a su probabilidad de explotación. Seguido a esto un análisis del impacto que recibirían las organizaciones en caso de la materialización de una amenaza, y con todo este conjunto de información determinar a ciencia cierta cuales son los riesgos actuales de los activos de información.

Para la identificación de amenazas y fuentes de amenaza se hace una clasificación de amenazas ambientales y medioambientales, de entorno y humanas, dividiéndose estas últimas e voluntarias e involuntarias. Sin entrar en definiciones, aquí se nombran:

Ambientales: Fuego, agua, desastre natural.

Entorno: Fuego, agua, contaminación, contaminación electromagnética, fallos físico-lógicos, interrupciones de suministro de energía, cambios climáticos, cortes de intercomunicación, interrupción de servicios y suministros esenciales, y degradación temporal.

Humanas:

- **Involuntarias:** Errores de personal, errores de monitoreo, errores de configuración, deficiencia en definición de roles, difusión involuntaria de software malicioso, fugas de información, alteración involuntaria, destrucción de información, divulgación de información, errores de mantenimiento y actualización, e indisponibilidad del personal.
- **Voluntarias:** Configuración manipulable, suplantación, privilegios excedidos, usos imprevistos, difusión de código malicioso, acceso no autorizado, análisis de tráfico, repudio, intercepción, alteración, información falsa, corrupción de activos, destrucción de activos, divulgación inapropiada, denegación de servicios, robo, ataques destructivos, invasión de instalaciones, indisponibilidad intencionada del personal, extorsión, e ingeniería social.

Adicionalmente a las amenazas humanas voluntarias, se identifican las personas que podrían ser posibles violadores de la seguridad y sus motivaciones y capacidades. Sin profundizar en definiciones, se listaron los siguientes:

Fuentes de amenaza de personal: Hackers y crackers, criminales informáticos, espías industriales, personal interno, vándalos, saboteadores y terroristas.

En este punto se siguió desarrollando la Guía Metodológica a la par de las plantillas. Una de las plantillas propuestas es la del listado de amenazas, donde aparte de su definición y clasificación, se sugirió que llevaran también un *Código* de identificación único, esto con el fin de poder llevar el dato de la amenaza a la plantilla de cálculo de riesgo inherente, sin tener que gastar mucho espacio en su caracterización. Es mejor una referencia a la lista.

La valoración de las vulnerabilidades se realiza sobre la probabilidad de que estas puedan ser explotadas. La frecuencia de explotación puede depender de factores como la capacidad y motivación que tenga la fuente de amenaza, la efectividad de los controles y la naturaleza misma de la amenaza. De acuerdo a esto se definió una escala de probabilidad de explotación medida cualitativamente en tiempo y cuantitativamente en porcentajes así:

Magnitud de frecuencia	Descripción	Probabilidad de materialización	Valor
Altamente Frecuente	Incidente ocurrido reincidentemente con controles previos ya establecidos	Muy Alta	81% - 100%
Muy Frecuente	Incidente ocurrido reincidentemente sin controles previos establecidos.	Alta	61% - 80%
Frecuente	Incidente presentado por segunda vez con controles previamente definidos.	Media	41% - 60%
Poco Frecuente	Incidente presentado por segunda vez sin controles previamente definidos.	Baja	21% - 40%
Raramente Frecuente	Incidente presentado una sola vez	Muy Baja	0% - 20%

Tabla 2: Tabla de valoración de vulnerabilidades

La explotación de una vulnerabilidad generará sobre la organización un impacto, que es la afectación negativa por causa de la materialización de la amenaza. Para medir este nivel de impacto, la Guía Metodológica se centró también en los 7 principios de la seguridad de la información, definiendo el impacto para cada uno de ellos y una escala de valoración. Se añadió también el impacto sobre la imagen de la organización y el impacto económico.

Las valoraciones del impacto se definieron de la siguiente manera:

Pérdida de Integridad

Pérdida de Integridad		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Todo el activo y su información dañados
Alto	4	Gran cantidad de información importante del activo dañada
Medio	3	Gran cantidad de información del activo dañada
Bajo	2	Mínima información importante del activo dañada
Muy Bajo	1	Mínima información del activo dañada

Tabla 3: Tabla de valoración de impacto sobre la integridad

Pérdida de Disponibilidad

Perdida de disponibilidad		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Total Indisponibilidad del activo
Alto	4	Amplia indisponibilidad del activo fundamental
Medio	3	Amplia indisponibilidad del activo
Bajo	2	Mínima indisponibilidad del activo fundamental
Muy Bajo	1	Mínima indisponibilidad del activo

Tabla 4: Tabla de valoración de impacto sobre la disponibilidad

Pérdida de Confidencialidad

Pérdida de confidencialidad		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Toda la información revelada
Alto	4	Importante cantidad de información sensible revelada
Medio	3	Importante cantidad de información revelada
Bajo	2	Mínima información sensible revelada
Muy Bajo	1	Mínima información revelada

Tabla 5: Tabla de valoración de impacto sobre la confidencialidad

Impacto por deficiencias en la autenticación

Afectaciones por deficiencia en la autenticación		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Total suplantación de otros usuarios
Alto	4	Importante acceso a privilegios críticos de otros usuarios
Medio	3	Importante acceso a privilegios de otros usuarios
Bajo	2	Mínimo acceso a privilegios críticos de otros usuarios
Muy Bajo	1	Mínimo acceso a privilegios de otros usuarios

Tabla 6: Tabla de valoración de impacto sobre la autenticación

Impacto por deficiencias en la autorización

Afectaciones por deficiencia en la autorización		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Total falta de definición de roles y privilegios
Alto	4	Deficiene definición de roles y privilegios
Medio	3	Definición incompleta de roles y privilegios
Bajo	2	Buena definición de roles y privilegio
Muy Bajo	1	Total definición de roles y privilegios

Tabla 7: Tabla de valoración de impacto sobre la autorización

Impacto por deficiencias en la no repudiación

Afectaciones por deficiencia en la No repudiación		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Total escasez de registros de actividad, acciones y accesos
Alto	4	Deficiente registro de actividad, acciones y accesos
Medio	3	Registro ineficiente o incompleto de actividad, acciones y accesos
Bajo	2	Buen registro de actividad, acciones y accesos
Muy Bajo	1	Registro óptimo de actividades, acciones y accesos

Tabla 8: Tabla de valoración de impacto sobre la no repudiación

Impacto por deficiencias en la observancia

Afectaciones por deficiencia en la observancia		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Tiempos de vida de registros de actividad, acciones y accesos no defiidos
Alto	4	Tiempos de vida de registros de actividad, acciones y accesos aleatorios
Medio	3	Tiempos de vida de registros de actividad, acciones y accesos insuficientes
Bajo	2	Tiempos de vida de registros de actividad, acciones y accesos suficientes pero no ajustados a la norma
Muy Bajo	1	Tiempos de vida de registros de actividad, acciones y accesos ajustados a la norma

Tabla 9: Tabla de valoración de impacto sobre la observancia

Pérdida de imagen

Pérdida de imagen		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Desprestigio del negocio
Alto	4	Alta pérdida de imagen y credibilidad
Medio	3	Importante pérdida de imagen
Bajo	2	Moderada pérdida de imagen
Muy Bajo	1	Mínima pérdida de imagen

Tabla 10: Tabla de valoración de impacto sobre la imagen

Pérdidas económicas

Pérdidas económicas		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Costo de reposición total del activo + Costo de recuperación de información asociada al activo + Costos adicionales posibles*
Alto	4	Costo de restauración del activo + Costo de recuperación de la información asociada al activo.
Medio	3	Costo de restauración del activo + Costo de restauración de la información asociada al activo
Bajo	2	Costo de restauración del activo
Muy Bajo	1	Costo de restauración de la información asociada al activo.
*Un costo adicional puede ser la pérdida económica ligada al tiempo de inactividad de un sistema		

Tabla 11: Tabla de valoración de impacto sobre el capital

Es importante recordar que las escalas definidas en este capítulo no son definitivas e inmutables. En la medida en que los equipos encargados de la seguridad y la administración de riesgos requieran modificar estas escalas o sus valores, el ejercicio de administración de riesgos se mantiene sobre las necesidades específicas de cada organización.

La probabilidad de ocurrencia y el impacto son las variables sobre las cuales se calcula el riesgo inherente, cálculo que sustenta esta segunda fase. Una vez obtenidos los valores para estas variables se procedió a definir la escala y la matriz de determinación de riesgo inherente. Para esto se asignaron valores numéricos a las escalas Muy Alto, Alto, Medio, Bajo y Muy Bajo definidas en las secciones anteriores para la Probabilidad de ocurrencia y el Impacto tras la materialización. De éste modo:

- **Probabilidad:** Muy Alta = 100, Alta = 80, Media = 60, Baja = 40, Muy Baja = 20
- **Impacto:** Muy Alto = 5, Alto = 4, Medio = 3, Bajo = 2, Muy Bajo = 1

Nuevamente se aclara que estas escalas son una propuesta que puede ser modificada de acuerdo a los intereses y necesidades de cada organización. Algunos podrían no definir una relación de 5X5 sino una de 3X3 o incluso relaciones no cuadradas como 4X5.

Ya que a diferencia de la mayoría de las metodologías en el mercado que sólo hacen un análisis de impacto sobre los principios de confidencialidad, integridad y disponibilidad, eligiendo el valor de impacto entre el mayor de ellos o promediando, y que la Guía Metodológica busca hacer un análisis sobre todos los principios; para el cálculo del impacto total que determine el riesgo se determinó que se promediarían los valores de todos, y que en caso de que no aplique el impacto a algún principio este suma 0 y no divide.
Los valores numéricos de la probabilidad vienen dados por el máximo del rango de probabilidad para cada valor cualitativo de la escala.

Así, la matriz de riesgo inherente quedó definida de la siguiente manera:

Matriz de determinación de Riesgo Inherente		Impacto				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Probabilidad (Max %)	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo
	20	1 x 20 = 20	2 x 20 = 40	3 x 20 = 60	4 x 20 = 80	5 x 20 = 100
	Bajo	Muy Bajo	Bajo	Bajo	Medio	Medio
	40	1 x 40 = 40	2 x 40 = 80	3 x 40 = 120	4 x 40 = 160	5 x 40 = 200
	Medio	Muy Bajo	Bajo	Medio	Medio	Alto
	60	1 x 60 = 60	2 x 60 = 160	3 x 60 = 180	4 x 60 = 240	5 x 60 = 300
	Alto	Bajo	Medio	Medio	Alto	Muy Alto
	80	1 x 80 = 80	2 x 80 = 180	3 x 80 = 240	4 x 80 = 320	5 x 80 = 400
	Muy Alto	Bajo	Medio	Alto	Muy Alto	Muy Alto
	100	1 x 100 = 100	2 x 100 = 200	3 x 100 = 300	4 x 100 = 400	5 x 100 = 500

Tabla 12: Matriz de niveles de riesgo inherente

Para los siguientes valores de las escalas definidos más profundamente en la Guía:

Riesgo	Valor Mínimo	Valor Máximo
Muy Bajo	1	60
Bajo	61	160
Medio	161	240
Alto	241	310
Muy Alto	311	500

Tabla 13: Tabla de valoración de riesgo inherente.

Fase III: Desarrollo de controles y mitigación de riesgos.

Esta tercera fase es la que entre ya fuertemente a darle su carácter de guía de aseguramiento físico a la Guía Metodológica. Ya habiendo dado las herramientas a la organización para conocer el estado actual de sus riesgos se procedió a hacer una exposición detallada de los controles de seguridad física que pueden implementar para mejorar los niveles de riesgo obtenidos.

Para la definición de controles primero se expuso una clasificación generalmente aceptada y definida por la mayoría de metodologías de controles de seguridad técnicos, operativos y de administración. Posterior a esto se decidió hacer una definición puntual de controles desde diferentes necesidades y puntos de observación. De este modo se definieron 3 grandes grupos de controles de seguridad física que van acercándose cada uno a un nivel menor de abstracción, yendo de lo grande y general, a lo pequeño y específico.

Estos son los 3 grandes grupos que se definieron para analizar la seguridad física y sus controles:

- Análisis de círculos concéntricos de la seguridad física
- Análisis para la seguridad física sobre instalaciones o edificios
- Análisis para la seguridad física sobre el entorno de los activos de información y la seguridad física sobre los activos de información

El primero de estos análisis, el de círculos concéntricos, busca analizar la seguridad física de la organización en el entorno de todas sus áreas: desde las que colindan con la calle y el vecindario hasta las zonas que alojan un determinado activo de información: Así se definieron observaciones y controles para 5 áreas o círculos perimétricos de fuera hacia dentro:

- El vecindario
- La barrera perimetral
- Las áreas internas abiertas
- Los muros periféricos de las instalaciones
- Las áreas internas del edificio

Entrando al análisis de las instalaciones y los edificios puntualmente donde se miran los criterios y controles para los siguientes aspectos de las instalaciones:

- El suministro eléctrico
- El acceso físico a las instalaciones
- Los controles contra incendios e incidentes
- El control de warchalking

Y por último, en el menor nivel de abstracción se dio paso al análisis sobre los entornos de los activos de información y los activos mismos, proponiendo observaciones y controles para:

- Centros de cómputo
- Conexiones y cableado
- Equipos remotos
- Equipos de escritorio
- Telecomunicaciones y equipos de comunicaciones
- Sistemas de vigilancia y alarma

Con esto se trató de cubrir de la mejor manera posible a todas las áreas y consideraciones posibles sobre la seguridad física para dar como herramienta controles posibles para cualquier tipo de vulnerabilidad que pueda representar una amenaza en el entorno de la seguridad física de las organizaciones. De igual modo se desarrolló una plantilla para el listado de controles, que al igual que la de listado de amenazas, propone una codificación de cada control para asociarlo más fácilmente a un activo de información específico.

Ya con esta información es posible seguir el proceso de administración de riesgos dando paso a la mitigación o la toma de decisiones frente a los riesgos.

Frente a los riesgos encontrados en el análisis de gestión, la literatura especializada propone diferentes alternativas para lidiar con ellos. Las más usuales son:

- ✓ Tolerar el riesgo, lo que implica no implementar controles y asumir el impacto caso tal que la amenaza se materialice.
- ✓ Tratar el riesgo, que implica adoptar los controles definidos anteriormente que tengan lugar para mitigar los riesgos inherentes de la organización.
- ✓ Transferir el riesgo, que implica buscar que un tercero asuma o comparta el riesgo con la organización.

- ✓ Terminar el riesgo, que es una decisión drástica cuando el impacto del riesgo es muy grande y no puede ser mitigado, transferido ni mucho menos tolerado. Terminar el riesgo implica finalizar la actividad para poder eliminar la posibilidad del riesgo.

En caso de que la opción sea mitigar o tratar el riesgo se decidió un esquema de mitigación cuyo riesgo residual esté en función del riesgo inherente y la efectividad de los controles seleccionados. De este modo las variables para calcular el riesgo residual de la organización son el riesgo inherente ya calculado y la efectividad de los controles adoptados. Se definió la siguiente escala de efectividad de controles, recordando nuevament6e que no es una camisa de fuerza para las organizaciones.

Escala Cualitativa	Escala Cuantitativa	Descripción
Deficiente	5	No existe o no se ha implementado el control
Malo	4	El control existe pero no es efecivo
Aceptable	3	El control existe y es efectivo pero no se aplica debidamente
Bueno	2	El control se aplica debidamente pero no es 100% eectivo
Excelente	1	El control se aplica debidamente y es 100% eectivo

Tabla 14: Tabla de valoración de eficiencia de controles

Y sobre esto se definió, con las mismas escalas de 5X5 del riesgo inherente, la matriz del riesgo residual.

Matriz de determinación de Riesgo Residual		**Nivel de Riesgo Inherente**				
		Muy Bajo	**Bajo**	**Medio**	**Alto**	**Muy Alto**
		1	2	3	4	5
Efectividad de Controles	**Excelente**	**Muy Bajo**	**Muy Bajo**	**Muy Bajo**	**Muy Bajo**	**Muy Bajo**
	1	1 x 1 = 1	2 x 1 = 2	3 x 1 = 3	4 x 1 = 4	5 x 1 = 5
	Bueno	**Muy Bajo**	**Muy Bajo**	**Muy Bajo**	**Muy Bajo**	**Bajo**
	2	1 x 2 = 2	2 x 2 = 4	3 x 2 = 6	4 x 2 = 8	5 x 2 = 10
	Aceptable	**Muy Bajo**	**Muy Bajo**	**Muy Bajo**	**Bajo**	**Medio**
	3	1 x 3 = 3	2 x 3 = 6	3 x 3 = 9	4 x 3 = 12	5 x 3 = 15
	Malo	**Muy Bajo**	**Muy Bajo**	**Bajo**	**Medio**	**Alto**
	4	1 x 4 = 4	2 x 4 = 8	3 x 4 = 12	4 x 4 = 16	5 x 4 = 20
	Deficiente	**Muy Bajo**	**Bajo**	**Medio**	**Alto**	**Muy Alto**
	5	1 x 5 = 5	2 x 5 = 10	3 x 5 = 15	4 x 5 = 20	5 x 5= 25

Tabla 15: Matriz de riesgo residual

Con la siguiente escala de valores:

Riesgo	Valor Mínimo	Valor Máximo
Muy Bajo	1	9
Bajo	10	14
Medio	15	19
Alto	20	24
Muy Alto	25	

Tabla 16: Tabla de valoración de escalas de riesgo residual

Fase IV: Revisión y documentación

En esta última fase se siguieron los lineamientos de los principales estándares y metodologías recalcando la importancia de la documentación de todo análisis y todos los resultados con el fin de que sean un insumo para reevaluar la gestión de riesgos, revisarla periódicamente, corregirla, actualizarla, etc.

3.4 Fase IV: Evaluación de la guía metodológica

3.4.1 Introducción

En esta nueva fase se dio cumplimiento al último objetivo específico de la propuesta que plantea que la guía metodológica propuesta debe ser validada por medio de un caso de estudio en una empresa nacional del sector financiero, esto con el fin de validar su utilidad y asertividad para el proceso de administración de riesgos de la seguridad física de la información.

3.4.2 Contacto y contrato con la organización

La organización en la que se puso a prueba la Guía metodológica es una empresa del sector financiero colombiano con la cual se pudo establecer contacto por la cercanía que tiene, a nivel de negocios y a nivel fundacional y misional con la Universidad Javeriana y con la Compañía de Jesús

Por tratarse de asuntos relacionados con la seguridad de la información, procesos críticos, misión de negocio y finanzas, se firmó entre la empresa y quien presenta el presente trabajo de grado un acuerdo de confidencialidad sobre toda la información a la cual el realizador pueda acceder por su grado de sensibilidad. Por este motivo y para los efectos netamente académicos del presente documento se omitirá el nombre de la organización, su localización geográfica y cualquier otra información que pueda facilitar su identificación y ubicación.

Por tratarse justamente de la aplicación de una guía metodológica, este proceso se hizo del modo en que está consignado en ella. De este modo, la aplicación de la guía se hizo sobre las 4 fases anteriormente mencionadas en esta memoria y registradas en la Guía metodológica.

3.4.3 Fase I: Caracterización de la organización

La organización es una empresa de seguros de vida y riesgos laborales que cuenta con 786 empleados directos a lo largo de todo el territorio nacional. Su labor económica se basa por un lado en el aseguramiento de riesgos laborales a empresas y venta de seguros de vida a particulares. En el área de riesgos laborales realiza labores de prevención de accidentes, tratamiento médico y aseguramiento contra accidentes laborales.

En el marco de la validación de la Guía Metodológica, diseñada para ser implementada por Pequeñas y Medianas Empresas (PyMes) que en la legislación colombiana se definen como empresas con una planta de personal de 11 a 50 trabajadores y un total de activos por valor entre 501 y 5000 Salarios Mínimos Legales Vigentes (SMLV) en el caso de las pequeñas, y una planta de personal entre 51 y 20 trabajadores y activos totales entre 5001 y 30000 SMLV.[9]; Se definió un universo de activos representativos de la empresa de aplicación para simular los activos de una PyMe, dado que la empresa seleccionada Supera en número de empleados a la definición de mediana empresa. Esto se da en acuerdo con la empresa para la aplicación de la guía y por el esquema de organización y levantamiento de activos que la organización maneja de forma adecuada y acorde a lo propuesto en la guía metodológica.

3.4.3.1 Contexto jurídico

En el contexto jurídico, la organización se encuentra obligada por ley a cumplir con las disposiciones de seguridad de la información pautadas por la Superintendencia Financiera de Colombia además de sus disposiciones internas
Estas normativas son:

- La circular externa 042 de octubre de 2012[10]
- Las disposiciones al riesgo operativo SARO[11]
- Las instrucciones relativas a la administración del riesgo de lavado de activos y financiación del terrorismo SARLAFT[12]
- Estándar ISO 27001[13]

- Política general de activos de información
- Funciones del comité de auditoría
- Código de gobierno corporativo

3.4.3.2 Levantamiento de activos

Respecto al levantamiento de activos de información de la organización, se había realizado ya un proceso de gestión de riesgos en el año 2010. Dicho proceso jamás llegó a completarse o avanzarse y de él sólo quedó un levantamiento de activos de información por procesos de negocio.

Según las prácticas usuales de la seguridad de la información, los registros de activos de información deben revisarse con una periodicidad usual de un año, por lo que la información con la que se cuenta es ya desactualizada.

Para ajustarse a las condiciones de cronograma que tiene este trabajo de grado y revisando junto al cliente este levantamiento de activos se acordó entre las partes aplicar la Guía metodológica a uno de los macroprocesos definidos en la empresa que tuviera un fuerte nivel de impacto en el negocio de la organización. La fase de levantamiento de activos fue entonces una actualización completa de levantamiento de 2010 sobre el macroproceso de administración de ingresos que se realizó con el equipo encargado de hacerlo en dicho año.

Sobre la base de este macroproceso como una muestra del universo de macroprocesos y activos de información de la empresa se aplicaría la guía metodológica culminando el proceso que se dejara incompleto y sin resultados en el año 2010.

Los activos de este macroproceso son de 3 tipos:

- Lógicos: Registros virtuales que se guardan en un servidor tras su procesamiento en el portal web de la empresa
- Físicos: Estos son el soporte real y jurídico de la información. Aun cuando se ha sistematizado el proceso para que los registros queden almacenados virtualmente, las exigencias de ley obligan a que haya un documento original en físico.
- Imágenes: Son el archivo escaneado del registro físico que es almacenado por un servidor y administrado por un tercero.

Para efectos de la demostración académica de este documento se muestra a continuación una muestra de los activos de información actualizados según lo especificado en la Guía metodológica y sus plantillas.

La codificación del activo es, para los casos siguientes "SI" por *Soportes de Información* seguido de un guion y un consecutivo empezando desde 1.

Soportes de información						
Codigo:	SI-001	**Nombre:**	SOLICITUD (DE LA EMPRESA) DE CONCILIACION DE SALDOS			
Descripción:	Solicitud de conciliación de saldos a clientes - Tiempo de retención: 10 años					
Propietario:	Gerente de operaciones					
Custodio:	Equipo archivo central					
Ubicación:	Archivo Central - Número de lote radicado				**Cantidad:**	-
Tipo:	Electrónico		Disco duro		Memoria USB	
			Disco virtual		Memoria Flash	
			CD ROM / DVD		Cinta/Diskette	
	No Electrónico	X	Impresión	X	Otro	

Tabla 17: Levantamiento activo de información SI-001

Soportes de información						
Codigo:	SI-002	**Nombre:**	SOLICITUD (DE LA EMPRESA) DE CONCILIACION DE SALDOS			
Descripción:	Solicitud de conciliación de saldos a clientes - Tiempo de retención: Permanente					
Propietario:	Gerente de operaciones					
Custodio:	DTI					
Ubicación:	Servidores - Número de radicado				**Cantidad:**	-
Tipo:	Electrónico	X	Disco duro	X	Memoria USB	
			Disco virtual		Memoria Flash	
			CD ROM / DVD		Cinta/Diskette	
	No Electrónico		Impresión		Otro	

Tabla 18: Levantamiento activo de información SI-002

Valoración de activos								
Codigo	SI-001	**Nombre**	SOLICITUD (DE LA EMPRESA) DE CONCILIACION DE SALDOS					
Evaluación		Muy Bajo	Bajo	Medio	Alto	Muy Alto	No aplica	**Tipo**
Criterios	Integridad					X		Público
	Disponibilidad			X				
	Confidencialidad			X				Privado
	Autenticación				X			X
	Autorización				X			Confidencial
	No repudiación					X		
	Observancia		X					Costo
Observaciones								$ -

Tabla 19: Valoración del activo de información SI-001

Valoración de activos								
Codigo	SI-002	**Nombre**	SOLICITUD (DE LA EMPRESA) DE CONCILIACION DE SALDOS					
Evaluación		Muy Bajo	Bajo	Medio	Alto	Muy Alto	No aplica	**Tipo**
Criterios	Integridad					X		Público
	Disponibilidad			X				
	Confidencialidad			X				Privado
	Autenticación				X			X
	Autorización				X			Confidencial
	No repudiación					X		
	Observancia		X					Costo
Observaciones								$ -

Tabla 20: Valoración del activo de información SI-002

3.4.4 Fase II: Gestión de riesgos

Para el proceso de gestión de riesgos se realizaron las visitas a las oficinas, el archivo central (lugar donde se guardan todos los archivos impresos) y el centro de cómputo.

Con respecto al centro de cómputo la organización está muy avanzada en políticas de seguridad ya que comparte ese mismo centro con otras organizaciones que son filiales del mismo grupo y son de mayor valor y envergadura como empresas.
En cuanto a las oficinas se encontraron algunas falencias al igual que en el archivo central.

Aquí se muestra lo encontrado. La siguiente lista muestra las amenazas encontradas en las visitas:

Lista de amenazas identificadas					
Código	Natural	Entorno	Humana		Fuente de amenaza / Descripción
			Involuntaria	Voluntaria	
TH-001			X		Destrucción del activo involuntariamente por un empleado distraido
TH-002			X		Divulgación inapropiada involuntariamente a un empleado que no tenga prvilegios de acceso
TH-003			X		Pérdida del activo involuntariamente
TH-004				X	Pérdida del activo por sustracción
TH-005		X			Degradación temporal por contaminación de polvo
TH-006		X			Degradación temporal por exposición a luz solar
TH-007		X			Destrucción del activo por fuego o agua
TH-008			X		Dificultad y demora en localizar el activo
TH-009				X	Acceso no autorizado a los activos
TH-010			X		Incapacidad de encontrar el activo por almacenamiento inadecuado de backup
TH-011			X		Vigilancia insuficiente

Tabla 21: Lista de amenazas

En las oficinas se encontró que no hay conciencia sobre el trato que se le debe dar a los archivos privados. En el caso de SI-001, antes de ser enviado al archivo central se encuentra en carpetas desordenadas por el piso junto a activos tales como reportes de siniestros o historias clínicas. No hay una organización por carpetas y estos documentos privados no se archivan bajo llave. Durante las horas del almuerzo quedan sin vigilancia y accesibles a todos los empleados.

En el caso del archivo central no existen medidas de seguridad para la conservación de los documentos. Más del 70% de los documentos allá almacenados no se encuentran en estibas sino en carpetas legajadoras sobre el piso o en estantes llenándose de polvo y expuestos a la luz solar. Se encontraron documentos ya en blanco por la degradación de la tinta. Hay muchos documentos pendientes de ser archivados por falta de identificadores. No existe diferenciación de áreas, no hay áreas restringidas para documentos de mayor relevancia. Todo está en la misma área. El acceso por las ventanas es muy sencillo, no tienen rejas ni cerraduras adecuadas. Ceden y abren a presión. El traslado de documentos de un lugar a otro es hecho por un empleado en su vehículo particular y ahí mueve documentos que son únicos al menos judicialmente.

En el edificio que aloja el Data center se encontró que hay cámaras de seguridad que no están funcionando y que las que funcionan no guardan las grabaciones el tiempo estipulado por la ley, reescribiendo archivos cada 2 meses.

Tomando las mediciones de impacto que se enuncian en la guía más las mediciones de probabilidad para las vulnerabilidades, y haciendo uso de la matriz de riesgo inherente obtenemos el siguiente resultado para el activo SI-001:

Determinación de Riesgo Inherente														
Codigo:	SI-001	**Nombre:**	SOLICITUD (DE LA EMPRESA) DE CONCILIACION DE SALDOS											
Codigo Amenaza	**Vulnerabilidad**		**Impacto**									**Probabilidad**	**Impacto total**	**Riesgo Inherente**
			Integridad	**Confidencialidad**	**Disponibilidad**	**Autenticación**	**Autorización**	**No repudiación**	**Observancia**	**Imagen**	**Dinero**			
TH-001	Activo regado por el piso sin clasificación ni custodia		4	4	4	0	3	4	0	2	0	30	4	120
TH-002	Activo regado por el piso sin clasificación ni custodia		1	5	4	3	4	3	0	1	0	10	3	30
TH-003	Activo regado por el piso sin clasificación ni custodia		2	5	5	5	5	3	0	1	0	30	3	90
TH-004	Activo regado por el piso sin clasificación ni custodia		2	5	5	5	5	3	3	3	0	10	4	40
TH-008	Activo regado por el piso sin clasificación ni custodia		0	2	4	2	0	3	3	0	0	40	3	120
TH-009	Activo regado por el piso sin clasificación ni custodia		1	4	3	5	2	4	0	0	0	30	3	90
TH-005	Activo mal almacenado en bodega. Sin protección contra polvo		5	0	4	0	0	0	3	0	0	50	4	200
TH-006	Activo expuesto directamente a la luz solar. Tinta de fax desvanecida.		5	0	4	0	0	0	3	0	0	10	4	40
TH-007	En cas de fuego o inundación la exposición es muy alta		5	0	5	0	0	0	3	0	0	10	4	40
TH-010	Mala o nula indexación. Activo no ubicado en su lugar		2	2	5	0	3	3	0	0	0	40	5	200
TH-011	Fácil penetración al almacén por puertas y ventanas. Pocas medidas		2	3	3	3	4	2	0	2	2	30	3	90
TH-004	Fácil penetración al almacén por puertas y ventanas. Pocas medidas de seguridad de ingreso.		3	5	5	2	0	0	2	4	0	10	4	40
TH-004	No hay medidas de seguridad para el traslado del documento.		3	5	5	2	0	0	2	2	0	10	3	30

Tabla 22: Cálculo de riesgo inherente para SI-001

3.4.5 Fase III: Desarrollo de controles y mitigación de riesgos:

De acuerdo a las visitas hechas a las distintas instalaciones de la empresa se proponen los siguientes controles para el tratamiento de los riesgos citados anteriormente.

Lista de controles sugeridos				
Código	Técnico	Administración	Operaivo	Descripción
CN-001		X		Flash informativos para los empleados recordando las políticas dentro de la oficina
CN-002	X			Digitalizar la información
CN-003			X	Muebles temporales para el almacenamiento de documentos en la oficina, mientras se hace la clasificación y se llevan al archivo central
CN-004	X			Empaquetar los documentos en bolsas plásticas y archivar estos paquetes en cajas
CN-005	X			Implementar el uso de estibas en el archivo central
CN-006	X			Poner a las evntanas una película protectora contra rayos solares
CN-007	X			Enrejar ventanas y mejorrar sus cerraduras
CN-008			X	Contratar un equipo auxiliar para el apoyo en el archivo. Agilización del proceso
CN-009	X			Utilizar una tipo de caja o estiba con mayor seguridad para los documentos catalogados
CN-010	X			Adaptar sistemas de almacenamiento de logs para que cumplan con los tiempos de almacenamiento mínimos

Tabla 23: Controles propuestos para la mitigación de riesgos de SI-001

Es importante señalar que el cálculo del riesgo residual depende completamente del riesgo inherente ya calculado y de la efectividad de los controles seleccionados. Para el caso práctico de la validación de esta guía la empresa es libre de aceptar o no las recomendaciones de control e implementarlas, y aun implementándolas, esa es una labor que requiere tiempo y recursos.

Por esto el proceso de administración de riesgos de la empresa cierra en este punto y pasa a la siguiente fase, dejando solo planteados los controles propuestos para la mitigación del riesgo inherente y dejando a la empresa la decisión de implementarlos o manejar el riesgo como consideren pertinente.

3.4.6 Fase IV: Revisión y documentación

Para el cumplimiento de esta cuarta y última fase, se desarrolló una reunión con el cliente para mostrarle las observaciones realizadas y los resultados obtenidos. En este punto terminó la interacción con el cliente y se dio finalización al proceso de aplicación de la Guía metodológica haciendo entrega al cliente de los resultados obtenidos, el informe detallado y por supuesto la Guía metodológica, que aunque propiedad de la universidad como proyecto de grado, se acordó podía ser entregada al cliente junto a los resultados como retribución a la gentil disposición y colaboración para el buen fin de este trabajo de grado.

4. CONCLUSIONES Y TRABAJOS FUTUROS

4.1 Conclusiones

El proceso de investigación de metodologías y referencias bibliográficas para el desarrollo del trabajo de grado se desarrolló satisfactoriamente en la medida en que su lectura y documentación fue indispensable insumo para el desarrollo de la Guía metodológica.

La guía se desarrolló sobre una sólida base teórica que le permite apreciarse como una nueva herramienta para la gestión de riesgos con énfasis en la seguridad física de la información, soportada por buenos estándares y literatura de renombre y amplio uso en la industria, en cuanto siempre serán importantes y vigentes las necesidades de avanzar más en el perfeccionamiento de la seguridad.

El desarrollo de todo el trabajo de grado se cumplió con un manejo muy estrecho de tiempo dado el volumen de trabajo que exigía para 192 horas. El proceso de aplicación de la guía debió acotarse para poder dar oportunidad de cumplir, por un lado con el compromiso adquirido con la organización, y por otro con la propuesta y los objetivos trazados para el desarrollo total de este trabajo.

Con el tiempo como barrera limitante para un desarrollo ideal de cualquier actividad o en este caso el desarrollo del trabajo de grado, siempre serán posibles mejoras y nuevos aporte para hacer de la Guía metodológica una herramienta más fuerte, corregida, ampliada y nutrida. Queda en manos de quien quiera continuar con este trabajo aportarle más y solidificarla como una herramienta que pueda empezar a ser utilizada ampliamente en la industria.

Por último puede concluirse que la experiencia de colocar a la Guía metodológica en la industria fue un proceso muy positivo que la reafirmó como una propuesta válida, útil y necesaria además de permitir al desarrollador de este trabajo de grado la oportunidad de salir a la industria a defender un producto propio, gran cierre del pregrado como la expresión máxima de la aprehensión de conocimientos sobre la ingeniería de sistemas y el trabajo relacionado con la ingeniería.

4.2 Trabajos futuros

Una vez tratado el tema de la administración de riesgos sobre la seguridad física, es posible ampliar más el espectro para avanzar hacia un nivel de abstracción mayor y desarrollar proyectos que innoven y desarrollen la actividad de la seguridad de la información.

Un posible trabajo futuro sería avanzar en el campo de la seguridad de la información con un proyecto sobre modelamiento y trabajo sobre consultoría en Sistemas de gestión de la seguridad de la información SGSI

Bibliografía

[1] P. F. Drucker, “Detrás de la revolución de la información,” *Rev. Factoría Oct.-Enero*, no. 13, 2001.
[2] S. NIST, “800-30,” *Risk Manag. Guide Inf. Technol. Syst.*, pp. 800–30, 2002.
[3] H. M. Treasury, “The Orange Book: management of risk–principles and concepts,” *Lond. HM Treas.*, 2004.
[4] C. S. de Administración Electrónica, *MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.-España. Fecha de consulta: 1 de abril de 2010*. .

[5] Almanza Junco, Ricardo Andrés, "Encuesta: Seguridad Informática en Colombia. Tendencias 2011-2012." 2012.
[6] M. Erbschloe, *Physical security for IT*. Access Online via Elsevier, 2004.
[7] D. Kushner, "The real story of stuxnet," *Spectr. IEEE*, vol. 50, no. 3, pp. 48–53, 2013.
[8] Congreso de la república, "Ley 1273 de 2009." 2009.
[9] Ministerio de Comercio, Industria y Turismo "MinCIT," "Definición Tamaño Empresarial Micro, Pequeña, Mediana o Grande." .
[10] Superintendencia Financiera de Colombia, "Circular Externa 042 de 2012." 04-Oct-2012.
[11] Superintendencia Financiera de Colombia, "Circular 041 de 2007. Reglas Relativas a la Administración del Riesgo Operativo." Jun-2007.
[12] Luís Fernando Merchán Gutiérrez, "'SARLAFT' Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo.".
[13] Instituto Colombiano deormas Técnicas y certificación ICONTEC N, "Norma Técnica NTC-ISO/IEC Colombiana 27001." 22-Mar-2006.

GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

CIS1310SD02

FELIPE BAYONA BORRERO

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C

2013

GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

CIS1310SD02

AUTOR
FELIPE BAYONA BORRERO

HTTP://PEGASUS.JAVERIANA.EDU.CO/~CIS1310SD02

DIRECTOR
ING. JOSHSUA JAMES GONZALEZ DIAZ

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C
2013

GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

Rector Magnífico

Padre Joaquín Emilio Sánchez García S.J.

Decano Académico Facultad de Ingeniería

Ingeniero Jorge Luís Sánchez Téllez

Decano del Medio Universitario Facultad de Ingeniería

Padre Sergio Bernal Restrepo S.J.

Director de la Carrera Ingeniería de Sistemas

Ingeniero German Alberto Chavarro Flórez

Director departamento Ingeniería de Sistemas

Ingeniero Rafael Andrés González Rivera

Tabla de contenido

Índice de tablas

Índice de ilustraciones

INTRODUCCIÓN

A través de los años, la humanidad se ha visto enfrentada a las diferentes revoluciones que han proporcionado un desarrollo en muchos aspectos, como lo son el social, económico, intelectual, etc. La revolución que hoy enfrentamos es aquella que se conoce como *La revolución de la Información"*, donde se llega a proponer hasta en marcos legales jurídicos, que la información se convierte en uno de los activos más valiosos en nuestra era, tanto así que llega a considerarse un bien jurídico tutelable. [1]

Para dicho activo, sin importar el estado en el que se encuentre (Digital, Documental, Físico, Conocimiento), su proceso de aseguramiento no llega a ser tan sencillo teniendo en cuenta que en nuestro mundo, donde la tecnología avanza a pasos agigantados, constantes y frecuentes, siempre en busca de mejorar la productividad e impulsar las industrias, no se quedan atrás las estrategias y motivaciones para buscar los puntos débiles de estos avances y explotarlos para intereses malintencionados.

Cada nuevo día la información cobra más relevancia como conocimiento y propiedad que genera y sustenta valor en los negocios, y sobre esta base los esfuerzos de las organizaciones por asegurarla de manera adecuada se vuelve una labor primordial y esencial en la búsqueda de mantener el negocio.

Muchas veces la seguridad física es relegada a un segundo plano por la falsa concepción de que el soporte tecnológico de la información se concentra en sus manifestaciones intangibles informáticas y no tanto en los soportes tangibles. Así muchas organizaciones enfocan la mayoría de sus esfuerzos en seguridad en los últimos avances en defensa contra software malicioso, intrusiones y estabilidad informática dejando de lado las exigencias de seguridad que deben tener los equipos que soportan el funcionamiento de estos sistemas lógicos.

Por tal motivo se piensa en la iniciativa de que la guía metodológica muestre y ofrezca a las organizaciones una visión completa desde su análisis hasta su implementación de seguridad física de sus activos de información y hagan una correcta administración de los riesgos asociados a su entorno y funcionamiento físicos como un factor decisivo en su estudio integral de la seguridad en pro de un óptimo desarrollo del negocio y su misión.

PROPÓSITO

La gestión de riesgos de los activos de información es un proceso iterativo que debe ajustarse constantemente a los avances de la tecnología. El propósito de esta guía metodológica es dar a la organización una base procedimental paso a paso, donde se llegue a realizar un proceso cíclico, brindados bases sólidas para la toma de decisiones en implementación de controles en cuanto a la seguridad física.

ALCANCE

El alcance de la presente guía es brindar un conjunto de procedimientos que permitan a las pequeñas y medianas empresas (Pymes) administrar los riesgos de seguridad que se ciernan sobre sus activos de información en su entorno y cualidades físicas. La guía se basa en una serie de instrucciones y plantillas que seguidas en su respectivo orden ayudarán a las organizaciones a hacer un levantamiento de sus activos de información, la identificación de sus riesgos, la implementación de sus controles de mitigación y la decisión sobre el riesgo residual que sobre ellos subsistan.

ESQUEMA PROPUESTO PARA LA ADMINISTRACIÓN DE RIESGOS

El modelo que se propone a continuación pretende proporcionar una herramienta para la identificación y gestión de riesgos correspondiente a aspectos de la seguridad física dentro de la compañía. Este consiste en una serie de pasos secuenciales que permitirán al equipo encargado de la evaluación de riesgos y seguridad de IT llevar el proceso de manera más ordenada y eficiente. Es importante también recordar que este proceso no es de realización única, debe por el contrario ser un proceso iterativo, de constante revisión y actualización, y que debe articularse con todas las áreas de la compañía y sus equipos de trabajo.

La fase de análisis de riesgos pretende establecer una lista de riesgos clasificados según su prioridad, determinada por la probabilidad de materialización de un riesgo particular y la magnitud del impacto que genere su ocurrencia. De este modo, una prioridad alta es dada a un riesgo que resulta ser más crítico y por esta misma naturaleza debe ser mitigado con mayor prontitud sin olvidar el costo relacionado con dicha medida. Para determinar el impacto de materialización de un

riesgo vale la pena plantearse preguntas del estilo: ¿qué puede, cómo y por qué puede ocurrir? ¿Qué tan malo puede ser y a quienes afectaría?

El modelo que se propone ayudará a evaluar y gestionar cualquier riesgo independientemente de su prioridad. Es importante aclarar que la guía no representa una "camisa de fuerza" frente a los procedimientos y definiciones para la administración de riesgos: Cada organización puede adaptar las propuestas de la presente guía de acuerdo a sus particularidades y necesidades.

Una vez identificados, analizados y priorizados los riesgos se procede a establecer los mecanismos de respuesta ante ellos que permitan direccionarlos en la mayor medida posible. Es importante recordar que sólo en contadas ocasiones es posible la mitigación del 100% del riesgo.

Así entonces el proceso se basará, en primera instancia, en un levantamiento de información que permitirá conocer los activos de información de la compañía para luego identificar los posibles riesgos a los que se ven expuestos. Tras esto se elabora un análisis de dichos riesgos de acuerdo a las variables de probabilidad e impacto y por medio de una escala se priorizan los mismos para por último diseñar las tácticas propias de mitigación.

Todo el anterior proceso debe documentarse debidamente en cada etapa para así poder hacer un seguimiento del proceso de administración de riesgos, que por su carácter iterativo debe estar en constante revisión y actualización. Así mismo todos estos resultados deben verse reflejados en el diseño de políticas de seguridad que describan las bases y procedimientos para todos los trabajadores de la compañía que tengan relación con sus activos de información. ¡La seguridad es un trabajo conjunto y mancomunado de esfuerzos de todos en la compañía!

El siguiente gráfico muestra el esquema propuesto para la administración de riesgos:

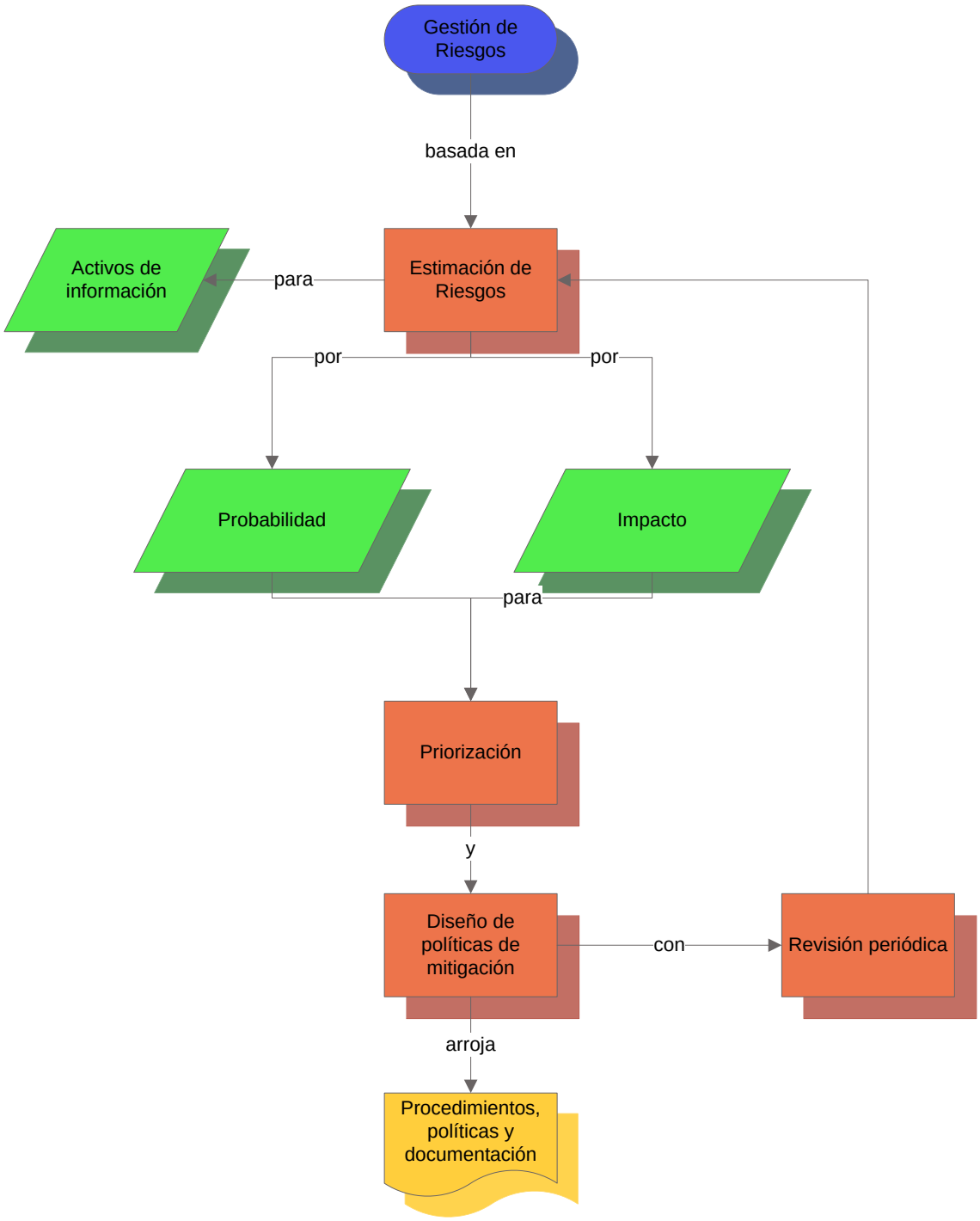


Figura 1: Esquema de administración de riesgos

GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

Introducción

La guía ofrecerá una serie de consideraciones, procedimientos y herramientas que ayuden en la administración y gestión de riesgos de seguridad física para los departamentos asociados a tecnologías de información. Dentro del marco presentado en el capítulo anterior nos dispondremos entonces a detallar puntualmente la secuencia de labores que nos permitirán hacer un análisis completo de riesgos, para así poder diseñar e implementar las políticas necesarias para la prevención y mitigación de los mismos respecto a la seguridad física de la organización.

La guía toma diferentes referencias en cuanto al análisis de riesgos, como lo son el Orange Book,[2] la Guía para manejo de riesgos NIST 800-30,[3] la metodología MAGERIT [4] y otras metodologías mundialmente reconocidas, donde luego de un análisis, se llegan a abstraer y generar los procedimientos para el análisis de riesgos enfocados hacia la seguridad física.

El lenguaje de la siguiente guía es similar a la mayoría de guías metodológicas que se encuentran en el mercado, y plantea una serie de consideraciones ordenadas para llevar a cabo el proceso de administración de riesgos de la seguridad física sin definir un esquema paso a paso. Las consideraciones de escalas numéricas y cuantitativas quedan a discreción del personal encargado de su implementación así como demás consideraciones que consideren propias para su negocio.

Es importante resaltar que la aplicación y manipulación de esta guía debe estar a cargo de personal con conocimientos y experiencia en el área, en busca de la óptima comprensión y aplicación de la misma. Y de igual modo poder desarrollar y adaptar su desarrollo a las condiciones propias de cada organización en particular.

¿Por qué una Guía para Pymes?

Las Pequeñas y Medianas Empresas (PyMEs) son de especial relevancia ya que representan a la industria emergente que desarrolla diferentes sectores económicos de la industria nacional en

comparación con las Grandes empresas multinacionales, esparcidas por todo el planeta y con capitales muy elevados, o las Micro empresas, que suelen ser negocios nacientes y de bajo capital. Para estas últimas el problema de la seguridad de la información es respectivamente, bien un asunto muy desarrollado por grandes equipos y profunda planeación e integración de sucursales y sistemas, o un asunto menor dado que la cantidad de información manejada puede estar en manos de pocas personas y no se cuenta con mayores prácticas de sistematización y documentación abundante.

Para las empresas pequeñas y medianas de todo el país el aseguramiento de su información es un reto cada vez más exigente y necesario en la medida en que desarrollan su avance: Un incremento de clientes y pedidos, un mayor cubrimiento de sus servicios, una expansión hacia otras zonas o sucursales, una integración de negocios, etc. representan un desafío de seguridad de la información para que los riesgos y posibles perjuicios no crezcan a la misma razón que el negocio.

La legislación colombiana define a una Pequeña Empresa como una empresa con planta de personal de 11 a 50 personas y un total de activos por valor entre 501 y 5000 Salarios Mínimos Legales Vigentes (SMLV), y a una Mediana Empresa como una empresa con planta de personal entre 51 y 20 trabajadores y activos totales entre 5001 y 30000 SMLV [5].

Fases de desarrollo

A continuación se presenta la guía metodológica objetivo de este trabajo de investigación, la cual sigue el esquema presentado anteriormente. La guía define 4 fases principales para su total aplicación:

V. Fase I: Caracterización de la organización.
VI. Fase II: Gestión de riesgos.
VII. Fase III: Desarrollo de controles y Mitigación de riesgos.
VIII. Fase IV: Revisión y documentación.

Dentro de las fases se encuentran definiciones técnicas para establecer un lenguaje conceptual común, las indicaciones y observaciones para cada fase, y un ejemplo de aplicación de cada fase para facilitar la implementación.

Principios de la seguridad de la información

La gestión de riesgos de esta guía metodológica girará alrededor de los 7 principios de la seguridad de la información; así, todas sus fases encargadas del direccionamiento de los riesgos tendrán un punto de referencia sólido para la evaluación de sus funciones y utilidad sobre la base de los consensos principales sobre los principios a los que debe apuntar la seguridad de la información.

Así entonces, se presenta la definición de los 7 principios de la seguridad de la información según la Organización Internacional de estandarización ISO en su estándar ISO/IEC 27002: [6]

- **Integridad:** Garantiza la exactitud de la información y que siempre sea completa. Es decir, que la información válida que se registró, o la estructura original o válidamente configurada del activo se mantiene como fue dispuesta por quien está autorizado.
- **Confidencialidad:** Garantiza que la información solamente es accesible a las personas autorizadas para tener acceso. Esto incluye que no sea interceptada, vista, accedida o modificada por usuarios no autorizados.
- **Disponibilidad:** Garantiza que los usuarios puedan tener acceso a la información en el momento requerido. Es decir que los activos de información están disponibles para los usuarios autorizados cada vez que estos los requieran.
- **Autenticación:** Garantiza que quien solicita un acceso es quien dice ser. Es decir que se corrobora que los usuarios que solicitan acceder a activos de información corresponden en la dupla ser-identificación.
- **Autorización:** Garantiza que alguien o algo acceda únicamente a lo que se le es permitido. Es decir que cualquier usuario que cuente con diferentes permisos sobre activos de información sólo pueda acceder a los permitidos por sus privilegios.
- **No repudiación:** Garantiza que quien genera un evento válidamente, no puede retractarse. Esto para llevar un seguimiento de acciones de los usuarios para saber quién hizo qué y que no pueda negarlo u ocultarlo.
- **Observancia:** Garantiza el adecuado funcionamiento de la seguridad. Es decir que las políticas y procedimientos son seguidos según lo especificado y que se cumplen las medidas de seguridad y funcionan los sistemas.

Es importante señalar que si bien, desde el punto de vista ideal, un escenario deseado en cuanto a estos principios de la seguridad de la información es alcanzar cada uno de estos en mayor grado de

aseguramiento, desde el punto de vista real llega a ser una labor titánica, sumando el hecho de que la posible optimización de alguno de estos podría llegar afectar directamente unos u otros aspectos de tecnología de la información, como lo son rendimiento, escalabilidad de los sistemas, flexibilidad, etc.

Una buena labor de aseguramiento se basa en un análisis cuantitativo como cualitativo de los riesgos, como en la identificación de los principios regentes sobre el activo de información.

1. Fase I: Caracterización de la organización

Esta primera fase pretende hacer una caracterización integral de la organización para conocer cuáles son sus procesos y activos ligados a proteger, cuales deben priorizarse de acuerdo a la criticidad que tenga su rol en la misión y objetivos de la organización, y cuáles son los controles y políticas existentes para la gestión de riesgos y el aseguramiento físico de la organización.

1.1 Identificación de activos

La persona o las personas que estén a cargo de la administración de riesgos deben, en primera instancia, recolectar toda la información referente a la organización, sus activos y sistemas que puede clasificarse de la siguiente manera: [3] En el documento anexo de plantillas, en la sección 2, se encuentran las plantillas sugeridas para el levantamiento de los activos de información bajo los criterios que se describirán a continuación.

- Activos físicos o hardware
- Licencias y programas o software
- Interfaces de los sistemas como por ejemplo la conectividad externa e interna
- Información y datos
- Personal que utiliza y da soporte a los sistemas
- Misión de los sistemas
- Información crítica para el negocio
- Los requerimientos de los sistemas
- Entorno de seguridad física, como la seguridad en la periferia.

De acuerdo al interés de esta guía metodológica, se presenta la clasificación de activos que correspondan a activos de información y sistemas físicos. [4]

1.1.1 Información General

- **Información crítica:** Aquí encontramos, por un lado, los activos de información que son vitales para el buen curso de la organización de modo tal que su daño o falta afectaría el buen desarrollo de las actividades de ésta. Aquí deben identificarse los recursos necesarios para que la organización se recupere en situación de emergencia, los que permitan desarrollar y reconstruir los procesos críticos, y también los que sustentan la legalidad del funcionamiento y las finanzas de la organización.

- **Datos de personal:** Es importante identificar la información sobre personas físicas que trabajen o no en la organización. Por ley de Habeas Data el manejo que se le dé a esta información debe estar estrictamente vigilado y regulado, y al organización debe asegurar la disponibilidad y actualización de ésta.

- **Información confidencial:** Aquí se haya la información que está sometida a restricciones de acceso y distribución, es decir aquella cuya confidencialidad es relevante para el negocio

1.1.2 Información de funcionamiento

Si bien la información es un activo abstracto en la medida en que suele ser digital, no solo su seguridad lógica debe ser garantizada. El enfoque de esta guía es la del aseguramiento de los equipos y sistemas físicos que guardan la información digital, así como los activos de información propiamente físicos.

De cualquier modo identificar la información clave es importante en el levantamiento de activos físicos como un modo de discriminación sobre cuál debe ser el grado y la priorización de seguridad de los equipos que la almacenan.
Dentro de estos activos de información encontramos:

- **Ficheros:** Archivadores lógicos que almacenan toda la información digital. El conocimiento de qué información hay y cual es prioritaria o crítica ayuda a identificar los equipos cuya seguridad debe priorizarse.

- **Backups:** Son copias de respaldo de la información que la organización reconoce como más importante. Su almacenamiento suele tener unos equipos y un lugar particulares y su priorización es crítica en la medida que puede ayudar a restablecer a la organización o sus sistemas en caso de una falla crítica.

- **Datos de configuración:** Estos dato son críticos para la configuración, establecimiento y restablecimiento de sistemas lógicos y físicos que prestan servicios a la organización.

- **Datos de control de acceso y de verificación de credenciales:** Diferentes áreas o sistemas de la organización requieren diferentes permisos físicos y lógicos para ser accedidos por el personal. La información referente a las configuraciones de estos sistemas y sus datos de validación de personal son críticos. Aquí también se encuentra toda la información referente a las claves criptográficas, de cifrado, de firma, de autenticación, de verificación de la autenticación y demás.

- **Registros de actividad:** Comúnmente conocidos como *Logs*, los registros de actividad son información que ayuda al seguimiento de la trazabilidad sobre operaciones en los diferentes sistemas de la organización. Mucha de esta información puede estar sujeta a especificaciones de almacenamiento, mantenimiento, tiempo de almacenamiento, entre otros aspectos, por la legislación vigente.

- **Código fuente, ejecutables y datos de pruebas:** Muchas organizaciones hoy en día desarrolla sus propias herramientas informáticas, y la información de dichos desarrollos como lo son el código fuente, los archivos binarios de ejecución y los datos de pruebas están sujetos a la legislación de propiedad intelectual, además de configurarse como información crítica en la medida en que van siendo adaptados al funcionamiento orgánico del negocio.

1.1.3 Servicios

Los servicios que presta la empresa están en gran medida sustentados por sistemas informáticos. Una priorización de dichos servicios puede ayudar a una mejor priorización de seguridad de los equipos que los sustentan.
Dentro de estos servicios se pueden identificar:

- **Servicios internos:** Que abarcan a los usuarios de la propia organización (Telnet, Correo electrónico, bases de datos, ftp, servicios de directorio, gestión de accesos y privilegios, PKI) Aquí también se ubican las distintas herramientas software que la organización utiliza (Ofimática, sistemas operativos, antivirus, navegadores web, clientes y servidores de correo electrónico y bases de datos, máquinas virtuales, terminales, software propio y licenciado)

- **Servicios públicos:** Los que se prestan al público en general sin relación contractual. (página web de la organización)

- **Servicios a usuarios externos.** Para personas con una relación contractual.

1.1.4 Hardware

Aquí encontramos los equipos que soportan directa o indirectamente los servicios que se prestan en la organización y los repositorios temporales o permanentes de los datos. Se pueden clasificar de la siguiente manera:

- **Hosts grandes:** Estos equipos suelen soportar informáticamente a la organización. Suelen ser servidores grandes que requieren un lugar de almacenamiento específico y acondicionado. Son los de menor cantidad y mayor costo, y suelen ser de más difícil reemplazo en caso de destrucción.

- **Hosts medios:** Suelen ser varios y el costo, tanto económico como de mantenimiento y reemplazo, es medio. Imponen algunos requerimientos en su entorno de operación pero no tan específicos como los grandes No son de difícil reemplazo en caso de destrucción

- **Hosts PC:** Suelen ser muy mayores en cantidad y sus requerimientos de entorno son mínimos. Su costo de compra, mantenimiento y reposición es relativamente bajo y son fácilmente reemplazables.

- **Hosts móviles:** Se clasifican como equipos de informática personal. Son fácilmente transportables y no requieren del entorno empresarial para funcional. Son de fácil reemplazo y no suelen portar información valiosa en sus propios recursos sino consultarla de sistemas remotos. Pueden ser teléfonos móviles, agendas electrónica, tabletas y similares.

- **Hosts virtuales:** Son equipos que se alojan fueran de la compañía y a los cuales ésta solo accede como un servicio. Dada esta cualidad de servicio las condiciones de seguridad de estos hosts recaen en responsabilidad sobre el propietario, quien los ofrece.

- **Hosts de backup:** Son equipos de respaldo. Pueden almacenar información concurrente para asegurarla o servir de soporte y apoyo "espejo" en respaldo a otros equipos que estén prestando servicios.

- **Hosts Periféricos:** Aquí se encuentras los equipos de impresión y escaneo. Pueden encontrase también equipos criptográficos.

- **Hosts de red:** Son los equipos encargados de la transmisión de datos (Módems, hubs, switches, routers, bridges, firewalls, puntos de acceso inalámbricos, telefonía IP)

1.1.5 Redes de comunicación

Aquí se encuentran tanto los servicios contratados a terceros como las infraestructuras de comunicación de los sistemas de la organización
Las redes de comunicación se soportan sobre los equipos de hardware de redes descritos en el punto inmediatamente anterior. Con diferentes equipos y arquitecturas, las diferentes redes pueden ser de telefonía, conexión punto a punto, radio, conexión inalámbrica, telefonía móvil, satelital, área local (LAN), área metropolitana (MAN) e internet.

1.1.6 Soportes de información

Los soportes de información son los medios físicos en los que se almacenan datos de forma permanente o temporal. Se clasifican en electrónicos y no electrónicos

- **Electrónicos:** Estos son los dispositivos que almacenan información virtual (Discos duros, discos virtuales, diskettes, CD-ROM, memorias USB, DVD, cintas magnéticas, tarjetas de memoria)

- **No electrónicos:** Contienen información tangible (Material impreso)

1.1.7 Equipos auxiliares

Aquí se encuentran los diferentes equipos que pueden o no servir de soporte a los sistemas de la organización, estando o no relacionados con datos. Se encuentran:
Equipos de alimentación (como fuentes de alimentación eléctrica, UPS, generadores eléctricos), equipos de calefacción o acondicionamiento de aire y clima, el cableado (eléctrico o de fibra óptica), los suministros esenciales de la organización, equipos de replicación o destrucción de soportes de información, todo el mobiliario de la organización, cajas de seguridad). Aquí también se ubican todos los equipos electrónicos y no electrónicos que apoyan la seguridad de la organización; estos pueden o no estar conectados a una red pero no se clasifican como tales porque su función no es transportar información del negocio (cámaras de seguridad, torniquetes de ingreso, lectores de tarjetas de acceso, sensores biométricos, etc.)

1.1.8 Instalaciones

Se refiere a las instalaciones de la organización donde se alojan los sistemas de información, de comunicaciones y el personal. Aquí están el edificio, sus diferentes zonas y cuartos con diferentes condiciones de entorno cada uno, puertas, barreras perimetrales, las instalaciones de respaldo, y los vehículos de la organización.

1.1.9 Personal

Aquí se describe al personal que interactúa con la organización y sus sistemas

- **Personal externos:** Puede tratarse de clientes, visitantes, proveedores, subcontratistas etc.

- **Personal internos:** Los trabajadores de planta de la organización (operarios, directivos, etc.)

- **Personal de administración:** Son personal interno, que dado el interés de esta guía, se clasifica independientemente por estar encargados de velar por el buen funcionamiento y seguridad de los sistemas y activos de información de la organización. Aquí están los administradores de redes y comunicaciones, de sistemas, de bases de datos, y de soporte. Adicionalmente se cuenta aquí el equipo encargado de la seguridad que abarca desde el personal de vigilancia hasta el de mantenimiento, configuración y manejo de equipos de seguridad y redes.

1.2 Técnicas de levantamiento de información

- **Formatos de clasificación:** De acuerdo a la clasificación anteriormente presentada de los activos, una documentación ordenada y clara de este levantamiento es vital para continuar con el proceso de gestión de riesgos.

- **Cuestionarios:** Tras una identificación clara de los empleados de la empresa y sus respectivos roles tanto en el manejo de la seguridad como en la manipulación y responsabilidad sobre la información y los activos críticos, el diseño de un cuestionario adecuado puede ayudar a obtener información relevante sobre la organización y sus sistemas.

- **Entrevistas:** Pueden ser muy útiles para recolectar información importante sobre la empresa y sus sistemas. Entrevistar a empleados clave sobre su visión de la empresa y su seguridad además de los riesgos que pueden observar en su cotidianidad en el ambiente físico de la empresa y las costumbres de los demás empleados y su operación dentro de la empresa, puede brindar una pauta clave sobre los principales riesgos que puedan presentarse. Para compañías donde los estudios y políticas de seguridad no se han diseñado

aun o están en etapa de diseño, las entrevistas son ejercicios 'cara a cara' de levantamiento de información que a la vez puede proveer la oportunidad de evaluar el entorno físico en que la empresa opera.

La siguiente es una entrevista recomendada para el jefe de control interno o de sistemas para el levantamiento inicial de la información de la organización en el marco de su caracterización.

Preguntas Base al personal de la organización para la aplicación de la Guía Metodológica
¿Cuál es la misión y visión de la organización?
¿Cuál es la estructura organizacional de la organización? ¿Organigrama? ¿Directivos de áreas?
¿Cuál es el marco legal al cual está sujeta la organización en cuanto a seguridad de la información?
¿Cual es la normativa interna respecto a la seguridad de la información?
¿Con que sistemas, físicos y lógicos, cuenta la organización y quienes son los encargados de cada uno? (Instalaciones, almacenes, Centros de cómputo, oficinas, etc)
¿Cómo se relacionan dichos sistemas, a nivel físico y lógico, con la misión organizacional y su negocio?
¿De qué importancia son dichos sistemas?
¿Cuál es la necesidad de disponibilidad de todos los sistemas, físicos y lógicos, para el funcionamiento correcto de la organización?
¿Qué información, tanto entrante como saliente, es fundamental, tanto en sistemas físicos como lógicos, para el correcto funcionamiento de la organización?
¿Qué información es generada, procesada, consumida, guardada y recuperada por cada área usando tanto sistemas físicos como lógicos?
¿Cuáles son los caminos de flujo de la información dentro de la organización de acuerdo a sus procesos e interacción tanto con sistemas físicos como lógicos?
¿Qué tipo de información se está moviendo allí? (de personal, financiera, investigación, marketing, etc)
¿Cuál es la clasificación de sensibilidad de la información por áreas, procesos o sistemas?
De acuerdoa los niveles de sensibilidad ¿Cuál es el personal o usuarios autorizados para acceder la información tanto de sistemas físicos como lógicos?
¿Dónde exactamente se procesa y almacena la información?
¿Cuál es el potencial impacto a la organización si se presenta un incidente de seguridad que afecte la integridad, confidencialidad o disponibilidad de la información de sus áreas, procesos o sistemas tanto físicos como lógicos?
¿Cuáles son las pautas organizacionales sobre la integridad y disponibilidad de la información?
¿Cuál es el máximo tiempo de caida de sistemas o indisponibilidad de la información tanto en sus áreas, procesos o sistemas físicos y lógicos que la organización puede tolerar?
¿Puede un mal funcionamiento, tanto de seguridad como de procesos, en algun sistema tanto físico como lógico, conducir a la muerte o a problemas de salud graves de cualquiera de los empleados o usuarios del negocio?

Tabla 24: Entrevista para la caracterización de la organización

- **Revisión de documentación:** Es importante revisar documentación interna o externa que ayude a conocer sobre qué campo se mueve el equipo de administración de riesgos en cuestiones de seguridad como documentos que especifican las políticas y directrices de la

empresa, documentación de los sistemas internos, y manuales de seguridad como reportes de auditorías, planes de seguridad, resultados de pruebas, reglamento interno de trabajo, contratos, etc. que pueden proveer buena información sobre los controles de seguridad usados y planeados para la empresa.

- **Uso de herramientas automatizadas:** Existen diferentes tipos de software encargados de escanear y monitorear deficiencias de seguridad y vulnerabilidades en sistemas. Son métodos técnicos que bien empleados pueden ser de gran utilidad levantando información.

1.2.1 Priorización de la información de activos levantada

Una vez levantada la información de todos los activos se procede a valorarlos y priorizarlos de acuerdo a su importancia para la organización y su negocio. Los criterios de evaluación son los 7 principios de la seguridad de la información descritos al inicio de este capítulo. Así, de acuerdo a cada uno se plantea la cuestión de cuál es la importancia y valor de chichos activos en el marco de cada principio. En dicho proceso cabe preguntarse sobre:

- ✓ **Integridad:** ¿Qué tanto se perjudicaría la organización con variaciones en la integridad de los activos?
- ✓ **Disponibilidad:** ¿Qué tanto se perjudicaría la organización si sus activos no estuvieran disponibles o parcialmente disponibles?
- ✓ **Confidencialidad: ¿**Qué tanto se perjudicaría la organización si sus activos de información fueran conocidos o utilizados por personas no autorizadas?
- ✓ **Autenticación:** ¿Qué tanto se perjudicaría la organización si el personal con el que cuenta o las personas que la frecuentan no son quienes dicen ser?
- ✓ **Autorización:** ¿Qué tanto se perjudicaría la organización si su personal o personas que la frecuentan obtuvieran accesos más allá de sus capacidades y permisos?
- ✓ **No repudiación:** ¿Qué tanto se perjudicaría la organización si no puede saber quién o quienes hicieron qué con sus activos e información?
- ✓ **Observancia:** ¿Qué tanto se perjudicaría la organización si no aplica controles de seguridad a sus activos?

Con estas preguntas clave se hace una aproximación inicial al valor de los activos en la empresa. Este valor se especificará más adelante al evaluar el impacto en la organización a la materialización de amenazas.

Esta valoración inicial puede medirse en una escala de 1 a 5, o de muy bajo a muy alto, de acuerdo a la evaluación cuantitativa o cualitativa y a su importancia para el negocio y la organización como se muestra a continuación:

Escala Cualitativa	Escala Cuantitativa	Descripción
Muy Bajo	1	Irrelevante para el negocio
bajo	2	Importancia menor o auxiliar para el negocio
Medio	3	Importante para el negocio
Alto	4	Altamente importante para el negocio
Muy Alto	5	De actuación crítica. El negocio depende fuertemente de él.

Tabla 25: Tabla de priorización de activos

Otra posible manera de valoración es la económica, aunque el valor económico no necesariamente va a estar relacionado siempre con el desarrollo directo del negocio. De cualquier forma, la determinación del valor material del bien es una labor que debe hacerse, en la medida de lo posible, independientemente de su relación directa o indirecta con el desarrollo del negocio de la organización. Esta distinción se presenta porque le valor material no siempre está ligado a la importancia. Por ejemplo unos diseños de implementación de un nuevo sistema de red, no valen como bits o planos impresos sino como información intelectual crítica para el negocio y muchas horas de trabajo y personal. En el documento anexo de plantillas, en la sección 3, se encuentra la plantilla sugerida para la evaluación y priorización de los activos de información según las especificaciones anteriores.

1.3 Resumen de la Fase I

La Fase I consta de las siguientes acciones:

Lista de chequeo acciones Fase I		
No.	**Actividad**	**¿Realizada?**
1	Diseñar entrevistas y cuestionarios que resullten adecuados para el tipo de personal a interactuar para obtener información de categorización de la organización. Partir sobre una base de investigación autónoma sobre la organización.	
2	Contactarse con una persona del área administrativa que pueda brindar información para una caracterización de la empresa (misión, visión, organigrama o áreas, principales funciones de cada una, etc.) Puede hacerse un cuestionario o una entrevista.	
3	Contactarse con el personal encargado de administrar la información o el área de TI y obtener un panorama sobre los sistemas existentes, la información, su flujo, usuarios, registros de incidentes, informes de auditoría y normas internas y legales que deban seguirse en la empresa. Puede hacerse un cuestionario o una entrevista.	
4	Con la información anteriormente obtenida, realizar un levantamiento de activos según las áreas de trabajo y zonas identificadas. Se recomienda hacerlas en compañía del personal encargado de cada activo para registrar observaciones y responsabilidades.	
5	Priorizar los activos de información identificados sobre los 7 Principios de la Seguridad de la Información como criterio.	

Tabla 26: Lista de chequeo acciones Fase I

2. Fase II: Gestión de Riesgos

Se da inicio a esta fase aclarando algunos conceptos claves para su propósito: [3]

- **Amenaza:** Es el potencial que tiene una fuente de amenazas para disparar accidentalmente o explotar deliberadamente una vulnerabilidad.

- **Fuente de amenaza:** Es una intención y un método dirigidos a la explotación intencional de una vulnerabilidad, o bien una situación y un método que pueden accidentalmente disparar una vulnerabilidad. Vale la pena resaltar que una fuente de amenaza no representa un riesgo en la medida en que no haya una vulnerabilidad qué explotar o disparar.

- **Vulnerabilidad:** Se entiende como una falla o una debilidad en procedimientos de seguridad, diseño, implementación o control sobre sistemas que se puede disparar accidentalmente o ejecutar intencionalmente, generando una brecha de seguridad o en una violación de sus políticas.

2.1 Identificación de amenazas y fuentes de amenaza

Una fuente de amenaza puede entenderse como cualquier circunstancia o evento con el potencial para causar un daño. Para la detección de fuentes de amenaza podemos mirar 3 posibles agrupaciones: En el documento anexo de plantillas, en la sección 4, se encuentra la plantilla sugerida para el registro de las amenazas de los activos de información según la clasificación que se describirá a continuación.

2.1.1 Amenazas Naturales o Medioambientales

Son las amenazas asociadas a catástrofes o accidentes naturales tales como inundaciones, terremotos, vientos fuertes, tormentas eléctricas, y eventos similares. Estas son algunas: [3]

- **Fuego:** El potencial de incendio que destruya los activos de información.
- **Agua:** El potencial de inundación que destruya los activos de información.
- **Desastre natural:** El potencial de que un incidente natural que se produce sin intervención humana destruya o perjudique los activos de información (Rayos, tormentas eléctricas, terremotos, huracanes y ciclones, tsunamis, deslizamiento de tierras, etc.)

2.1.2 Amenazas de entorno

Aquí se encuentran las amenazas que se pueden producir dentro del mismo entorno de la organización como fallas en los sistemas de suministro, de refrigeración, polución y corrosión, humedad, químicos, entre otros: Estos son algunos:

- **Fuego:** El potencial de incendio que destruya los activos de información.

- **Agua:** El potencial de inundaciones, escapes o fugas que destruyan los activos de información.
- **Contaminación:** El potencial de obstrucciones o daños mecánicos por polvo, suciedad, plagas, residuos alimenticios o industriales, etc. en los activos de información
- **Contaminación electromagnética:** El potencial de daño o desgaste por campos magnéticos o diferentes tipos de radiaciones electromagnéticas como radio, infrarrojos, ultravioleta, microondas, etc. sobre los activos de información.
- **Fallos físico-lógicos:** El potencial de que los sistemas informáticos o redes de comunicación fallen o resulten dañados por malfuncionamiento de los sistemas software o hardware que surjan en medio de la operación o vengan de fábrica.
- **Interrupción del suministro eléctrico:** El potencial de un corte de alimentación de potencia eléctrica a sistemas de información, redes de comunicación o instalaciones.
- **Cambios climáticos:** El potencial de cambios en la temperatura de los ambientes donde trabajan los sistemas de información y las redes, los lugares de almacenamiento de activos de información o las instalaciones donde trabaja el personal, excediendo los márgenes de trabajo de estos.. Puede ser exceso de calor, exceso de frio, exceso de humedad o falta de humedad.
- **Corte de intercomunicación:** El potencial cese de comunicación entre sistemas y el envío y recibo de datos.
- **Interrupción de servicios y suministros esenciales:** El potencial desabastecimiento de recursos esenciales para el buen funcionamiento o mantenimiento de los activos de información.
- **Degradación temporal:** El potencial de que soportes de información y de almacenamiento se degraden por el paso del tiempo.

2.1.3 Amenazas humanas

Aquí encontramos todos los eventos que puedan ser causados o desencadenados por las personas, tales como actos inintencionados o acciones deliberadas. Vale la pena hacer un poco más de énfasis en la determinación de éstas amenazas evaluando en profundidad las capacidades que tienen los empleados de acuerdo a sus roles y permisos dentro de la empresa, como los visitantes y personas externas, de causar daños o desencadenar un evento perjudicial. [4]

Dentro de las acciones involuntarias pueden encontrarse:

- **Errores de personal:** El potencial de equivocaciones cuando los usuarios usan los servicios o datos, o los administradores o personas con responsabilidades sobre sistemas erran en instalación u operación.
- **Errores de monitoreo:** El potencial de llevar un mal registro de actividades; registros incompletos o faltantes.
- **Errores de configuración:** El potencial de que las configuraciones y condiciones de trabajo de los sistemas no sean bien definidas a ellos.
- **Deficiencias en definición de roles:** El potencial de malos procedimientos o procedimientos no ejecutados cuando no se tiene claro el rol de cada persona en la organización.
- **Difusión involuntaria de software malicioso:** El potencial de que alguien ejecute y/o propague software malicioso en las redes y sistemas de la organización como troyanos, virus, gusanos, bots, etc.
- **Fugas de información:** El potencial de que la información pueda llegar a personas no autorizadas sin que esta se vea afectada en sí misma.
- **Alteración involuntaria:** El potencial de que la información sea alterada involuntariamente o se ingrese información incorrecta.
- **Destrucción de información:** El potencial de que la información o los activos de información asociados se pierdan o destruyan accidentalmente.
- **Divulgación de información:** El Potencial de divulgación inapropiada de información por indiscreción, incontinencia verbal, medios electrónicos o impresos.
- **Errores de mantenimiento o actualización:** El potencial de no actualizar a tiempo los equipos para que puedan seguirse utilizando más allá del tiempo nominal de uso.
- **Indisponibilidad del personal:** El potencial de pérdida de trabajo incompensable por ausencia, falta, incapacitación o incapacidad de llegar al lugar de trabajo del personal.

Las personas aparte de tener bastantes recursos para poder generar problemas o amenazas, pueden tener a su vez motivaciones, lo que los convierte en una fuente de amenaza potencialmente fuerte.
Identifiquemos algunas fuentes de amenaza de personal, sus motivaciones, y sus posibles acciones: [7]

- **Hackers y Crackers**: Sus motivaciones pueden ser muy variadas, pero además de los intereses económicos que puedan tener por la obtención o corrupción de información y sistemas, pueden tener motivaciones tales como el ego, la rebeldía o las exigencias y retos personales. Sus acciones pueden ser igualmente variadas y pueden ir desde inserciones no autorizadas a sistemas, pasando por intrusiones y vulneraciones de seguridad, hasta hurto, destrucción o modificación de información por medio de sistemas informáticos o por medio de otras personas (posiblemente empleados) por medio del engaño y la ingeniería social.

- **Criminales informáticos**: Los criminales informáticos además de tener todos los conocimientos y capacidades de un Hacker tienen además fuertes motivaciones monetarias, ideológicas y hasta políticas, y sus acciones pueden ser verdaderamente variadas. Con la intención de revelar información confidencial, destruirla, alterarla o comerciarla, estas personas pueden acechar sistemas cibernéticos, realizar actos fraudulentos como la suplantación, realizar sobornos o interceptaciones.

- **Espías industriales**: En ésta categoría podríamos encontrar a personas tanto de fuera como de adentro de la organización. La motivación económica como siempre puede estar presente, además de las ventajas competitivas que pueden obtenerse. El robo de información, la intrusión en la privacidad personal, la ingeniería social, la penetración a sistemas, el acceso no autorizado a sistemas y a información clasificada (como secretos industriales, ideas, proyectos por lanzar) son acciones que una persona trabajando para la competencia o para un buen postor podría utilizar colocando en grave riesgo procesos importantes dentro de la empresa. Un ataque de un espía puede fácilmente llegar a pasar desapercibidos ya que como su interés es principalmente el robo, no suelen causar daños. El estudio que hacen de las organizaciones es extenso y saben identificar muy bien y hacer seguimiento a sus objetos de interés dado su alto entrenamiento que les brinda además buenas técnicas de evasión a las fuerzas de la ley

- **Personal interno**: Diversas circunstancias pueden derivar en que un empleado interno de la empresa, con determinados niveles de acceso a la información o privilegios, pueda tornarse una fuente de amenaza para la seguridad. Desde empleados con poco entrenamiento, pasando por negligentes, enfadados, maliciosos, deshonestos, hasta empleados despedidos, pueden configurarse como serias amenazas. Tal como variados son sus perfiles así mismo variadas son sus motivaciones. Podríamos encontrar la curiosidad, el ego, la inteligencia, la

revancha, los intereses económicos y también las acciones sin dolo y omisiones. Sus posibles acciones son también un abanico amplio de opciones: El chantaje, los asaltos a otros empleados, la búsqueda de información sensible, el abuso de permisos y accesos y la extralimitación en los mismos, fraude y robo, el soborno, el ingreso de información errónea, distorsionada o falsificada, la interceptación, la inserción de códigos y software malicioso, la venta de información personal, desarrollar deliberadamente errores o fallos en los sistemas, sabotaje y acceso no autorizado a sistemas entre otras muchas acciones, podrían ser perpetradas por un trabajados no muy leal.

Éstos atacantes en particular pueden tener algunas ventajas para desarrollar sus acciones ilegales. Tienen conocimiento de las locaciones y están familiarizados con éstas y sus activos además de conocer el valor y la sensibilidad de éstos. Pueden también haber obtenido duplicaciones de llaves que les eran confiadas o conocer bien los códigos de acceso y alarmas. Podrían no estar trabajando solos y tener colaboración de otros empleados con información y accesos a otras áreas y tienen conocimiento de los hábitos dentro de la organización y los horarios en que ciertas áreas y puertas no están cerradas.

- **Vándalos:** Aunque si incidencia es menor muchas organizaciones han sufrido daños por actuaciones de vándalos. Los vándalos, que suelen llamarse vándalos casuales, son personas que no tienen ningún interés especial en la compañía o motivación particular para dañarla. Usualmente la ley no suele disuadirlos y sus conductas suelen ser por presiones grupales inducidas de tintes antisociales lo que los lleva a tener pocas consideraciones acerca de sus actos. Su actuación suele ser en grupos donde varios de sus miembros sirven como vigilantes o ‘campaneros’ para revisar la seguridad y alertar la presencia de fuerzas de seguridad o policiales, mientras otros destruyen sin mayor planeación. Los ataques de vándalos suelen ser destrucciones casuales y usualmente están dirigidas a blancos fáciles.

- **Saboteadores:** A diferencia de los vándalos, los actos de los saboteadores suelen ser de carácter más profesional y sí están dirigidos por intereses en contra de la empresa o sus aliadas. Muchos trabajan por intereses financieros, o incluso en tiempos de guerra por una combinación de intereses económicos y lealtad política. Los saboteadores a sueldo son personas muy bien entrenadas que están dispuestos a usar incendios o artefactos explosivos para causar daño. Dedican además abundante tiempo a investigar acerca de la organización y sus vulnerabilidades antes de lanzar un ataque, además de ser muy diestros en la evasión a policías o fuerzas de seguridad. Así mismo su daño es medido y calculado, por lo que las

vulnerabilidades que suelen atacar han sido estudiadas previamente y conocen el impacto de su daño

- **Terroristas:** La definición de terrorismo no es tan fácil como parece, pero algunas agencias de seguridad como las norteamericanas han coincidido en definir a los terroristas como grupos de odio, militantes extremistas, u organizaciones que se oponen a la existencia de la nación o la sociedad como están organizadas actualmente. Aunque son relativamente escasas las acciones de terroristas que han impactados a organizaciones cómo las que nos interesan en éste trabajo, cuando los ataques se presentan suelen ser de magnitudes muy fuertes en impacto y daño. Los terroristas se diferencian bastante de los otros agentes de amenaza que hemos mencionado hasta ahora pero pueden tener particulares ventajas a la hora de hacer daño: Son muy organizados y sus ataques son bien planeados y estudiados, suelen tomar medidas extremas y tienen poco reparo en la afectación a vidas humanas, no se ven disuadidos por la ley y suelen estar en contra de las normas impuestas en la sociedad contra las que suelen tomar retaliaciones.

Tomando en cuenta los perfiles mencionados, se pueden deducir algunas posibles amenazas que puedan ser ejecutadas intencionalmente por dichas personas. Entre ellas:

- **Configuración manipulable:** Potencial alteración de la configuración de los dispositivos y hosts para modificar accesos, registros de actividad, procedimientos, etc.
- **Suplantación:** Potencial de que un usuario con determinados accesos y privilegios sea suplantado por otro(s) individuo(s) para obtener los mismos privilegios sobre los activos.
- **Privilegios excedidos:** Potencial de que un usuario exceda sus privilegios y obtenga acceso a más información o posibilidades de las estipuladas.
- **Usos imprevistos:** Potencial de que un usuario utilice de manera indebida los activos a los que tiene acceso, esto para fines de intereses personales o en contra del negocio.
- **Difusión de código malicioso:** Potencial de que un usuario ingrese código malicioso como troyanos, espías, gusanos, etc. en los sistemas con el fin de cambiar condiciones de seguridad, de funcionamiento u obtención de información privilegiada.
- **Acceso no autorizado:** El potencial de que un usuario acceda a sistemas o zonas a las cuales no tiene autorización de acceso.

- **Análisis de tráfico:** El potencial de que un usuario realice observaciones y seguimiento a otros usuarios para conocer y prever sus comportamientos, horarios, costumbres y demás con el fin de utilizar esta información para explotar otras amenazas.
- **Repudio:** Potencial de que un usuario niegue sus acciones o actividades por falta de registro o seguimiento de estas.
- **Intercepción:** El potencial de que un usuario tenga acceso a información más allá de sus privilegios sin que esta información se vea alterada o no llegue a sus verdaderos destinatarios.
- **Alteración:** El potencial de que un usuario altere información, recursos, procesos o sistemas con el ánimo de obtener un beneficio personal o un perjuicio para el negocio.
- **Información falsa:** El potencial de que un usuario mueva información falsa en los otros usuarios de la organización con el fin de obtener beneficios personales o perjudicar el negocio.
- **Corrupción de activos:** El potencial de que un usuario degrade activos de información con el fin de obtener beneficio personal o perjuicio para el negocio.
- **Destrucción de activos:** El potencial de que un usuario elimine activos de información con el fin de obtener beneficio personal o perjuicio para el negocio.
- **Divulgación inapropiada:** El potencial de que un usuario divulgue información a la que tiene acceso a personas no autorizadas para conocerla.
- **Denegación de servicio:** El potencial de que, intencionalmente, un usuario manipule, alteres o desactive un sistema o equipo con la intención de explotar otras vulnerabilidades, obtener un beneficio propio o un perjuicio para la organización.
- **Robo:** El potencial de que un usuario sustraiga equipamiento o activos de información para perjuicio de la organización o el beneficio propio.
- **Ataques destructivos:** El potencial de que uno o varios usuarios desarrollen ataques vandálicos, militares o terroristas.
- **Invasión de instalaciones:** El potencial de que varios usuarios ingresen a las instalaciones, bien a zonas privilegiadas o bien a zonas públicas dificultando el correcto progreso del negocio. Pueden ser violentas o pacíficas, legales o ilegales.
- **Indisponibilidad intencionada del personal:** El potencial de pérdida de trabajo incompensable por absentismo laboral, huelgas, bloqueo de accesos, bajas injustificadas, etc.

- **Extorsión:** El potencial de que un usuario o grupo de usuarios realicen determinadas acciones impuestas por otros por medio de amenazas.
- **Ingeniería social:** El potencial de que un usuario o grupo de usuarios realicen determinadas acciones impuestas por otros por medio del abuso de su buena fe y confianza.

Adicionalmente a la anterior clasificación pueden hacerse diversas investigaciones sobre posibles historiales de ataques en el pasado, intromisiones, reportes de violaciones de normas de seguridad, reportes de incidentes, y entrevistas con administradores de los sistemas, personal de soporte técnico, y usuarios de los sistemas en general que los usen o estén sometidos a ellos durante el levantamiento de información, para así poder asegurar un sólido y completo análisis de amenazas.

2.2 Levantamiento de vulnerabilidades y fuentes de vulnerabilidad

Como ya se describió, una vulnerabilidad es una debilidad en un sistema, en un procedimiento de seguridad, en su concepción o en su desarrollo o bien una falencia en el ejercicio de los controles internos, que puede ser ejecutada de forma accidental o intencional causando un bache en la seguridad y la materialización de una amenaza. La meta ahora es desarrollar un análisis, lo más completo y detallado posible, de las vulnerabilidades físicas y del entorno de los activos de información de la organización que puedan ser explotadas por fuentes de amenaza.

Las vulnerabilidades pueden ser detectadas por diferentes medios que pueden clasificarse en la identificación de fuentes de vulnerabilidad, la ejecución de pruebas en busca de vulnerabilidades, y el diseño de listas de chequeo de requerimientos de seguridad. Usualmente la determinación de los recursos que deben usarse para el levantamiento de vulnerabilidades depende del estado actual de la seguridad en la empresa, sus avances e implementaciones. La revisión de las políticas ya implantadas, los planes de seguridad, la puesta a prueba de los productos e insumos asociados a los sistemas de seguridad, la revisión de pruebas y estudios antes realizados, entre varios más son fuentes principales de estudio de vulnerabilidades para empresas con mayor o menos implementación de equipos y políticas de seguridad.

Tanto las vulnerabilidades técnicas como las no técnicas pueden ser revisadas por los métodos de levantamiento de información descritos en la fase I. Adicionalmente, la revisión de casos y experiencias de otros actores de la industria puede ayudar a preparar buenas entrevistas y listas de

chequeo. La internet y el contacto con los servicios de soporte técnico de los proveedores de equipos pueden ayudar a mantenerlos actualizados de acuerdo a las últimas actualizaciones de software y licencias.

2.2.1 Testeo en busca de vulnerabilidades

Conociendo las fuentes de vulnerabilidad se puede proseguir con un testeo técnico de los sistemas de seguridad en busca de posibles brechas. Aquí podemos pensar principalmente en 3 procedimientos a seguir: [3]

- **Pruebas y evaluaciones de seguridad:** Las llamadas ST&E (Security Tests and Evaluations por sus siglas en inglés) son otra técnica que puede utilizarse para el levantamiento de vulnerabilidades durante el proceso de aseguramiento. Éstas incluyen el diseño y la implementación de planes de pruebas, como pruebas de equipos, procedimientos, resultados esperados; y se desarrollan con el objetivo de probar la efectividad de los mecanismos de control de seguridad aplicados ya a un ambiente de operación. El propósito es asegurarse de que los controles aplicados cumplen con las especificaciones de seguridad aprobadas para los equipos y sistemas, las políticas de la organización o los estándares industriales.

- **Pruebas de penetración:** Estas pruebas pueden complementar los procedimientos de revisión de los sistemas de seguridad. Su objetivo es probar los sistemas de seguridad desde el punto de vista de la fuente de amenaza y así identificar posibles falencias del esquema de protección de la organización. Pruebas lógicas o de ingeniería social pueden ser aplicadas para ambientes técnicos y no técnicos

2.3 Valoración de vulnerabilidades

Al igual que los activos de información se valorizan y priorizan de acuerdo a su valor de negocio, las vulnerabilidades tienen su valoración propia y está en función de la frecuencia de acontecimiento y la probabilidad de explotación de su amenaza respectiva. En el documento anexo de plantillas, en la sección 5, se encuentran la plantilla sugerida para el registro de las vulnerabilidades asociadas a cada amenaza de los activos de información y su valoración de ocurrencia según lo que se describirá a continuación.

Para derivar una buena escala que indique la probabilidad de que una vulnerabilidad potencial pueda ejecutarse en un ambiente de amenaza propicio, los siguientes factores deben ser tenidos en cuenta:

- ✓ La capacidad y motivación de la fuente de amenaza
- ✓ La naturaleza de la amenaza
- ✓ La existencia y la efectividad de los controles

De acuerdo a lo anterior podemos definir la siguiente escala:

Magnitud de frecuencia	Descripción	Probabilidad de materialización	Valor
Altamente Frecuente	Incidente ocurrido reincidentemente con controles previos ya establecidos	Muy Alta	81% - 100%
Muy Frecuente	Incidente ocurrido reincidentemente sin controles previos establecidos.	Alta	61% - 80%
Frecuente	Incidente presentado por segunda vez con controles previamente definidos.	Media	41% - 60%
Poco Frecuente	Incidente presentado por segunda vez sin controles previamente definidos.	Baja	21% - 40%
Raramente Frecuente	Incidente presentado una sola vez	Muy Baja	0% - 20%

Tabla 27: Tabla de valoración de vulnerabilidades

Como se verá más adelante, el riesgo inherente se calcula como una relación entre el impacto de la materialización de una amenaza y la probabilidad de dicha materialización. Dicho cálculo se hace por cada activo levantado de acuerdo a cada vulnerabilidad detectada para él.

Así entonces, la anterior valoración debe hacerse de acuerdo al levantamiento de incidentes recogidos durante la Fase I en la caracterización de la organización. Esta información permitirá saber si una vulnerabilidad ya ha sido explotada o identificada y si se han dispuesto o no controles para mitigarla. La probabilidad de materialización de una vulnerabilidad para un activo dependerá

entonces de un conocimiento histórico, ya sea documentado o no, de los incidentes ocurridos y su reincidencia en presencia o no de controles de mitigación lo que alterará dicha probabilidad.

2.3.1 Definición de niveles de probabilidad

La probabilidad de que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza puede verse, en base, clasificada de la siguiente manera: [4]

- **Probabilidad Muy Alta:** La motivación de la fuente de amenaza es muy fuerte y tiene la total capacidad para explotarla. Adicionalmente los controles para evitar dicha ejecución son inútiles.

- **Probabilidad Alta:** La motivación de la fuente de amenaza es fuerte y tiene la suficiente capacidad para explotarla. Adicionalmente los controles para evitar dicha ejecución son insuficientes.

- **Probabilidad Media:** Las motivaciones y facultades de la fuente de amenaza para ejecutar la vulnerabilidad están presentes, y los controles que pueden impedir dicha ejecución no son suficientemente confiables.

- **Probabilidad Baja:** Las motivaciones y facultades de la fuente de amenaza para ejecutar la vulnerabilidad están presentes, pero existen controles que pueden impedir de manera exitosa dicha ejecución.

- **Probabilidad Muy Baja:** La fuente de amenaza carece de la capacidad y motivación, o existen controles eficientes que pueden prevenir la explotación de la vulnerabilidad o cuanto menos impedirla exitosamente.

2.4 Análisis de impacto

Un siguiente paso en la medición y estimación de los riesgos es determinar el impacto adverso resultado de una explotación exitosa de una vulnerabilidad. En primera instancia es fundamental recolectar la siguiente información:

- Conocer muy bien la misión y el objeto de cada uno de los sistemas físicos que se encuentran en la compañía y que requieren ser asegurados. Así por ejemplo entender los procesos que desarrollan, a qué área de la organización ayudan, qué rol juegan dentro de todo el esquema de negocio empresarial, etc.

  .

- Conocer la criticidad de los sistemas. Es decir, conociendo su rol y misión se debe estimar cuál es su valor en términos de información, valor monetario, importancia para el buen desarrollo del negocio, etc.

- Conocer la sensibilidad de los sistemas, ligado al análisis efectuado sobre su vulnerabilidad frente a amenazas.

Esta información puede obtenerse de la documentación existente de la organización. De no existir puede desarrollarse un Análisis de Impactos del Negocio (BIA por sus siglas en inglés), un estudio que prioriza el nivel de impacto asociado al compromiso que puedan tener los activos de información de la organización basados en una evaluación cualitativa y cuantitativa de la sensibilidad y criticidad de dichos activos. Ésta evaluación prioriza la sensibilidad y la criticidad de los activos de información que soportan las misiones críticas del negocio.

Dicha sensibilidad puede ser determinada basándose en el nivel de protección requerido para mantener al día la disponibilidad, integridad y confidencialidad de la información que procesen estos sistemas y los sistemas mismos. Independientemente de los métodos usados para levantar esta información, es vital contar con el acompañamiento de las personas y equipos que son dueños o trabajan con estos sistemas, puesto que sobre ellos recae principalmente la responsabilidad de determinar el nivel de impacto, por lo que una entrevista puede ayudar a ensamblar el análisis.

2.4.1 Descripción de niveles generales de impacto

Al igual que con la determinación de la probabilidad, el impacto también puede medirse en una escala cualitativa definida esencialmente en impacto alto, medio o bajo: [3]

- **Impacto Alto:** Cuando una vulnerabilidad se ejecuta satisfactoriamente puede:
  - Resultar en un alto costo de pérdida de activos de información o recursos.

- Violar, dañar o impedir significativamente el buen desarrollo de la misión de la organización, su reputación o interés.
- Resultar en serias violaciones a la seguridad, tanto de la organización como de las personas, incluyendo inclusive heridas o muertes.

- **Impacto Medio:** Cuando una vulnerabilidad se ejecuta satisfactoriamente puede:
  - Resultar en un costo de pérdida de activos de información o recursos.
  - Violar, dañar o impedir el buen desarrollo de la misión de la organización, su reputación o interés.
  - Resultar en violaciones a la seguridad, tanto de la organización como de las personas.

- **Impacto Bajo: :** Cuando una vulnerabilidad se ejecuta satisfactoriamente puede:
  - Resultar en algún costo de pérdida de activos de información o recursos.
  - Afectar la misión, reputación o intereses de la organización

2.4.2 Descripción de niveles específicos de impacto

Recolectando lo anterior podemos definir el impacto adverso de un evento de seguridad en términos de la pérdida o degeneración de cualquiera o una combinación de los siguientes aspectos:

- A Nivel técnico: Afectación de acuerdo a los 7 principios de la seguridad de la información.
- A Nivel Organizacional: Perdida de Imagen y pérdidas económicas

A Nivel técnico se clasifica el impacto de acuerdo a los 7 principios de la seguridad de la información:

- **Pérdida de Integridad:** La integridad de sistemas y datos se refiere al requerimiento de protección de la información y los equipos de modificaciones indebidas. La integridad se pierde si accidental o intencionalmente se modifican la información o los sistemas de forma no autorizada. Su no corrección o prevención puede degenerar en uso de información inexacta o sistemas que no van estrictamente de acuerdo a su misión, lo que conllevaría a mala información para toma de decisiones, fraude, o inexactitudes. Además, la violación de

la integridad puede ser el primer paso para abrir una brecha de seguridad o un ataque efectivo en contra de la disponibilidad y la confidencialidad. Por estas razones la pérdida de integridad reduce o anula la garantía que se tiene sobre los sistemas afectados.

- **Pérdida de Disponibilidad:** Si un sistema de misión crítica no está disponible para sus usuarios finales la misión de la organización puede verse afectada. La pérdida de funcionalidad y eficiencia operativa puede desembocar en pérdidas de tiempo productivo o incluso en graves amenazas de seguridad asumiendo sistemas de seguridad afectados o deshabilitados.

- **Pérdida de Confidencialidad:** La confidencialidad se refiere a la protección de la revelación de sistemas en información. En el caso de sistemas físicos este principio de la seguridad puede entenderse junto al principio de Accesibilidad, referente a donde se encuentra el sistema y quién puede acceder a él. Pueden presentarse casos, sobre todo con equipos y sistemas que soportan misión crítica de la empresa, que su acceso sea limitado a un personal muy específico e incluso que su localización sea confidencial por temas de seguridad.

- **Afectaciones por deficiencia en la Autenticación:** Los métodos y políticas implementadas para una adecuada autenticación de usuarios es vital en el aseguramiento de otros principios de seguridad de la información como los tres mencionados arriba. Que una persona pueda llegar a suplantar a otra dentro de la organización y sus sistemas de autenticación podrá generar grandes brechas de seguridad con altos costos e impactos en la medida en que escalaría privilegios que están más allá de los que posee.

- **Afectaciones por deficiencia en la Autorización:** La no definición de roles claros para cada uno de los usuarios puede converger en que los límites de acceso de cada uno y sus responsabilidades con la seguridad no sean claros y la desprotección de la organización sea muy grande. Muchos principios de seguridad pueden ser fácilmente violados cuando la organización no ha gestionado bien el rol, las responsabilidades, las actividades, los recursos y los accesos que tiene el personal. No puede haber autenticación si no se he definido la autorización dado que es imposible saber quién es quién en la organización.

- **Afectaciones por Repudiación:** Sin el efectivo seguimiento de las actividades que se desarrollan dentro de la organización y sus procesos es muy difícil determinar la correspondencia de dichas acciones con sus realizadores. Además de una consistente autorización, el registro de actividades es fundamental para que ante un evento adverso pueda determinarse el responsable. Las fallas en el seguimiento y determinación de responsabilidad sobre las actividades no permite una identificación de la fuente de amenaza lo que prolonga su existencia y permite más posibles materializaciones de amenazas.

- **Afectaciones por Inobservancia:** Es inútil la definición de políticas de seguridad y la gestión de riesgos y direccionamiento de controles en la medida en que el proceso no sea constantemente revisado, valorado e incluso replanteado. La seguridad es una actividad constante, de vigilancia y estudio periódicos; sin ello la desactualización y las medidas previsibles y obsoletas se vuelven un factor adverso a la seguridad.

Algunos impactos tangibles pueden medirse cuantitativamente en pérdida de ingresos, costos de reparación de sistemas afectados, o el esfuerzo en trabajo adicional y no contemplado en la corrección de problemas causados por la explotación exitosa de una amenaza. El good will de la compañía, a pesar de ser un activo difícilmente cuantificable, es de capital importancia y un impacto a la imagen corporativa puede ser un profundo impacto económico a futuro en el desarrollo del negocio.
En los impactos no técnicos se encuentran: [4]

- **Pérdida de imagen:** Una afectación sobre el reconocimiento corporativo y la imagen y el prestigio de la marca suele ser devastadora para la organización porque afecta al esquema de negocio que representa. Esta afectación integral suele acarrear pérdidas económicas asociadas al desprestigio de la organización y su buen desarrollo de las actividades industriales.

- **Pérdidas económicas:** Estas pérdidas suelen ser el impacto colateral y último de cualquier vulneración de seguridad y posterior explotación de amenazas. El fin de toda organización es la rentabilidad de su negocio; un impacto económico puede llegar a determinar el futuro y la continuidad de una empresa.

En el caso de la definición del impacto hay que hacer una acotación importante sobre los análisis hechos sobre mediciones cualitativas y cuantitativas.
La principal ventaja de un análisis cuantitativo es el hecho de poder es que permite priorizar riesgos e identificar áreas de atención primordial o inmediata para el mejoramiento en el direccionamiento de las vulnerabilidades. Del modo contrario, la principal desventaja de un análisis cualitativo es que impide hacer una medición cuantitativa de la magnitud del impacto dificultando un análisis de coto-beneficio de los controles asociados.

La principal ventaja de un análisis cuantitativo de los impactos se encuentra en la posibilidad de hacer un estudio de costo-beneficio de los controles respecto a magnitudes cuantificables, pero así mismo una fuerte desventaja se encuentra en que, dependiendo de los rangos numéricos usados para la medida, el significado de los resultados numéricos puede no resultar claro exigiendo a su vez una interpretación cualitativa de la escala.

Para definir cuantitativamente el nivel de impacto ante la materialización de una amenaza por la explotación de una vulnerabilidad, se utiliza una escala cuantitativa de 1 a 5 para normalizar todos los posibles valores de impacto tanto para el impacto sobre efectos técnicos y no técnicos, aun cuando la descripción de cada uno de estos niveles para cada uno es diferente. Esto con el fin de utilizar una sola escala que permita igualar criterios de importancia para cada uno.
Aquí las descripciones de valoración de cada tipo de impacto:

Técnicos:

Pérdida de Integridad

Pérdida de Integridad		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Todo el activo y su información dañados
Alto	4	Gran cantidad de información importante del activo dañada
Medio	3	Gran cantidad de información del activo dañada
Bajo	2	Mínima información importante del activo dañada
Muy Bajo	1	Mínima información del activo dañada

Tabla 28: Tabla de valoración del impacto sobre la integridad

Para definir el impacto sobre la integridad de un activo explotada una vulnerabilidad, hay que enfocarse menos en la estructura física misma del activo, como en su información.

De este modo, por ejemplo, en caso de daño de un documento la pérdida recaería sobre la información que contiene más que la integridad del papel en que se encuentra; caso contrario del daño de un servidor donde habría una afectación en el equipo (un activo de hardware cuyo impacto de integridad representa más un impacto económico). Así entonces, la evaluación de integridad se hace considerando la importancia de la información y la cantidad afectada.

Pérdida de Disponibilidad

Perdida de disponibilidad		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Total Indisponibilidad del activo
Alto	4	Amplia indisponibilidad del activo fundamental
Medio	3	Amplia indisponibilidad del activo
Bajo	2	Mínima indisponibilidad del activo fundamental
Muy Bajo	1	Mínima indisponibilidad del activo

Tabla 29: Tabla de valoración del impacto sobre la disponibilidad

La evaluación de la disponibilidad recae en la valoración de la importancia del activo para el negocio. Así, cuando el activo es fundamental para el negocio su necesidad de disponibilidad es mayor.

Pérdida de Confidencialidad

Pérdida de confidencialidad		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Toda la información revelada
Alto	4	Importante cantidad de información sensible revelada
Medio	3	Importante cantidad de información revelada
Bajo	2	Mínima información sensible revelada
Muy Bajo	1	Mínima información revelada

Tabla 30: Tabla de valoración del impacto sobre la confidencialidad

La evaluación de la confidencialidad recae en la valoración de la sensibilidad del activo para el negocio. Así, cuando el activo es muy sensible en cuanto a su necesidad de confidencialidad para el negocio, la pérdida de dicha confidencialidad es más grave.

Impacto por deficiencias en la autenticación

Afectaciones por deficiencia en la autenticación		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Total suplantación de otros usuarios
Alto	4	Importante acceso a privilegios críticos de otros usuarios
Medio	3	Importante acceso a privilegios de otros usuarios
Bajo	2	Mínimo acceso a privilegios críticos de otros usuarios
Muy Bajo	1	Mínimo acceso a privilegios de otros usuarios

Tabla 31: Tabla de valoración de impacto sobre la autenticación

La evaluación de la autenticación en la valoración del nivel de acceso que se pueda obtener por suplantación de acuerdo a todas las facultades de acceso del usuario suplantado. Así, entre más privilegios se escalen por suplantación mayor es el impacto sobre la autenticación.

Impacto por deficiencias en la autorización

Afectaciones por deficiencia en la autorización		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Total falta de definición de roles y privilegios
Alto	4	Deficiene definición de roles y privilegios
Medio	3	Definición incompleta de roles y privilegios
Bajo	2	Buena definición de roles y privilegio
Muy Bajo	1	Total definición de roles y privilegios

Tabla 32: Tabla de valoración de impacto sobre la autorización

La evaluación de impacto sobre la autorización depende exclusivamente de qué tan avanzada esté la organización frente a la definición de roles, facultades y accesos de cada uno de sus usuarios. El impacto aumenta proporcional a la deficiencia en esa tarea.

Impacto por deficiencias en la no repudiación

Afectaciones por deficiencia en la No repudiación		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Total escasez de registros de actividad, acciones y accesos
Alto	4	Deficiente registro de actividad, acciones y accesos
Medio	3	Registro ineficiente o incompleto de actividad, acciones y accesos
Bajo	2	Buen registro de actividad, acciones y accesos
Muy Bajo	1	Registro óptimo de actividades, acciones y accesos

Tabla 33: Tabla de valoración de impacto sobre no repudiación

La evaluación de impacto sobre la deficiencia en la no repudiación depende exclusivamente de qué tan avanzada esté la organización frente a la tarea de documentación y registro de actividades y operaciones tanto informáticas como de usuarios. El impacto aumenta proporcional a la deficiencia en esa tarea.

Impacto por deficiencias en la observancia

Afectaciones por deficiencia en la observancia		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Tiempos de vida de registros de actividad, acciones y accesos no defiidos
Alto	4	Tiempos de vida de registros de actividad, acciones y accesos aleatorios
Medio	3	Tiempos de vida de registros de actividad, acciones y accesos insuficientes
Bajo	2	Tiempos de vida de registros de actividad, acciones y accesos suficientes pero no ajustados a la norma
Muy Bajo	1	Tiempos de vida de registros de actividad, acciones y accesos ajustados a la norma

Tabla 34: Tabla de valoración de impacto de observancia

La evaluación de impacto sobre la observancia depende exclusivamente de qué tan avanzada esté la organización frente al ajuste a la norma vigente sobre el registro de actividades, accesos y registros. El impacto aumenta proporcional a la deficiencia en esa tarea.

No Técnicos

Pérdida de imagen

Pérdida de imagen		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Desprestigio del negocio
Alto	4	Alta pérdida de imagen y credibilidad
Medio	3	Importante pérdida de imagen
Bajo	2	Moderada pérdida de imagen
Muy Bajo	1	Mínima pérdida de imagen

Tabla 35: Tabla de valoración del impacto sobre la imagen

La evaluación de impacto sobre la imagen está dada proporcionalmente al desprestigio o pérdida de imagen de la organización ante algún incidente.

Pérdidas económicas

Pérdidas económicas		
Valoración Cualitativa	Valoración Cuantitativa	Descripción
Muy Alto	5	Costo de reposición total del activo + Costo de recuperación de información asociada al activo + Costos adicionales posibles*
Alto	4	Costo de restauración del activo + Costo de recuperación de la información asociada al activo.
Medio	3	Costo de restauración del activo + Costo de restauración de la información asociada al activo
Bajo	2	Costo de restauración del activo
Muy Bajo	1	Costo de restauración de la información asociada al activo.
*Un costo adicional puede ser la pérdida económica ligada al tiempo de inactividad de un sistema		

Tabla 36: Tabla de valoración del impacto sobre el capital

La evaluación sobre las pérdidas económicas se calcula sobre el costo físico de un activo de información, el costo de la obtención de la información en caso de presentarse un incidente y los costos adicionales que puedan presentarse. Así, la pérdida económica es proporcional a la cantidad de rubros involucrados al presentarse un incidente más allá de una escala cuantitativa predefinida.
Así por ejemplo, en caso de incendio en una sala de cómputo, el nivel de impacto económico irá evaluado sobre el activo afectado y la gravedad del daño, por un lado físico y por otro lado la reparación de la integridad de la información que repose en el activo. Para el caso de un servidor de la sala el costo puede ser el de la reposición (en caso de pérdida total) o de reparación y a ello puede sumarse el costo de la recuperación de la información (traer el backup, recuperar la información del disco dañado, etc.). Adicionalmente pueden surgir otros rubros como multas, demoras y demás por falta de disponibilidad temporal de la información.

Es importante recordar que las escalas definidas en este capítulo no son definitivas e inmutables. En la medida en que los equipos encargados de la seguridad y la administración de riesgos requieran modificar estas escalas o sus valores, el ejercicio de administración de riesgos se mantiene sobre las necesidades específicas de cada organización.

2.5 Análisis de riesgos

Esta sección tiene como propósito medir el nivel de riesgo de los activos de información de la organización. La determinación del riesgo para una pareja particular Amenaza-vulnerabilidad puede ser expresada en función de:

- ✓ La probabilidad de una fuente de amenaza tratando de ejecutar una vulnerabilidad dada.
- ✓ La magnitud del impacto dada la ejecución de una vulnerabilidad por una fuente de amenaza.
- ✓ La utilidad de un control de seguridad planeado o existente para reducir o eliminar el riesgo.

En el documento anexo de plantillas, en la sección 5, se encuentran la plantilla sugerida para el registro del cálculo del Riesgo inherente de acuerdo al impacto y ocurrencia definidos anteriormente y sobre la escala de valoración que se describirá a continuación.

2.5.1 Matriz de niveles de riesgo inherente

La definición final de un riesgo inherente dado viene dado por la multiplicación de los rangos asociados a la probabilidad y al impacto, anteriormente definidos. En la siguiente matriz podemos ver las definiciones de nivel de riesgo de acuerdo a la anterior función. Es importante señalar que ésta definición es absolutamente subjetiva y sirve como base para explicar el concepto. De acuerdo a la organización los siguientes valores pueden cambiar; así, por ejemplo, podemos definir tanto para la probabilidad como para el impacto escalas que registren 3, 4 o 5 valores. Para el caso de esta guía se usará una matriz de 5x5 con los valores para probabilidad e impacto Muy Alto, Lato, Medio, Bajo, Muy Bajo. Se dice de riesgos inherentes en el marco de que sus mediciones se hacen sin tomar en cuenta los controles que los mitigan.

Para la siguiente matriz de riesgo inherente se asignan valores numéricos a las escalas Muy Alto, Alto, Medio, Bajo y Muy Bajo definidas en las secciones anteriores para la Probabilidad de ocurrencia y el Impacto tras la materialización. De éste modo:

- **Probabilidad:** Muy Alta = 100, Alta = 80, Media = 60, Baja = 40, Muy Baja = 20
- **Impacto:** Muy Alto = 5, Alto = 4, Medio = 3, Bajo = 2, Muy Bajo = 1

En caso de verse afectado más de un aspecto técnico o no técnico sus valores de impacto se promedian. Si no aplica su valor es 0 y no divide.

Los valores numéricos de la probabilidad vienen dados por el máximo del rango de probabilidad para cada valor cualitativo de la escala.

Así, la matriz de riesgo inherente queda definida de la siguiente manera:

Matriz de determinación de Riesgo Inherente		Impacto				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Probabilidad (Max %)	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo
	20	1 x 20 = 20	2 x 20 = 40	3 x 20 = 60	4 x 20 = 80	5 x 20 = 100
	Bajo	Muy Bajo	Bajo	Bajo	Medio	Medio
	40	1 x 40 = 40	2 x 40 = 80	3 x 40 = 120	4 x 40 = 160	5 x 40 = 200
	Medio	Muy Bajo	Bajo	Medio	Medio	Alto
	60	1 x 60 = 60	2 x 60 = 160	3 x 60 = 180	4 x 60 = 240	5 x 60 = 300
	Alto	Bajo	Medio	Medio	Alto	Muy Alto
	80	1 x 80 = 80	2 x 80 = 180	3 x 80 = 240	4 x 80 = 320	5 x 80 = 400
	Muy Alto	Bajo	Medio	Alto	Muy Alto	Muy Alto
	100	1 x 100 = 100	2 x 100 = 200	3 x 100 = 300	4 x 100 = 400	5 x 100 = 500

Tabla 37: Matriz de niveles de riesgo inherente

La escala de riesgo de la matriz es:

Riesgo	Valor Mínimo	Valor Máximo
Muy Bajo	1	60
Bajo	61	160
Medio	161	240
Alto	241	310
Muy Alto	311	500

Tabla 38: Tabla de valoración de escalas de riesgo inherente

2.5.2 Definición de niveles de riesgo inherente.

La anterior matriz nos muestra cualitativa y cuantitativamente los niveles de riesgo inherente a los que pueden estar expuestos los sistemas y activos de la organización en la escala Muy Alto, Alto, Medio, Bajo y Muy Bajo, en la medida en que una amenaza se ejecute. La Matriz también muestra indirectamente la priorización de las acciones que se deben tomar tras el análisis de riesgos.

Siguiendo con la descripción cualitativa de las escalas definidas, entendemos los riesgos de esta manera y las medidas que corresponden a cada uno:

- **Muy Alto Riesgo:** Si una observación es calificada como de muy alto riesgo, es de vital importancia corregir medidas inmediatamente ya que el nivel de riesgo es ***crítico***. En caso de recaer el riesgo sobre un sistema, se debe evaluar de acuerdo a la amenaza y la criticidad del sistema si debe seguir operando o detenerse por el tiempo que tarde tomar los correctivos necesarios.
- **Alto Riesgo:** Si una observación es calificada como de alto riesgo es importante corregir medidas a la mayor brevedad posible ya que el nivel de riesgo es ***grave***. En caso de recaer el riesgo sobre un sistema éste puede seguir operando, pero un plan de acciones de corrección debe ser puesto en marcha a la brevedad posible.
- **Mediano Riesgo:** Si una observación es evaluada como de mediano riesgo, las acciones correctivas son necesarias y un plan debe ser desarrollado para implementar dichas acciones en un periodo razonable de tiempo.
- **Bajo Riesgo:** Si una observación es evaluada como de bajo riesgo, el responsable del sistema o los activos implicados debe determinar las acciones correctivas que aún faltan por ser tomadas.
- **Muy Bajo Riesgo:** Si una observación es evaluada como de muy bajo riesgo, el responsable del sistema o de los activos implicados debe determinar si vale la pena proponer o ampliar controles, o decidir aceptar el riesgo. Más adelante detallaremos cómo asumir un riesgo es siempre una posibilidad en la medida en que el riesgo nunca es cero.

2.6 Resumen de la Fase II

La Fase II consta de las siguientes acciones:

Lista de chequeo acciones Fase II		
No.	**Actividad**	**¿Realizada?**
1	Conociendo la información de los activos a proteger y la categorización de la organización se identifican las amenazas existentes para los activos de acuerdo a la lista de amenazas.	
2	Una vez identificadas y registradas las amenazas se hace el levantamiento de las vulnerabilidades que podrían llevar a la explotación de una amenaza.	
3	Ya conocidas las vulnerabilidades, basándose en la información histórica recaudada en la categorización de la empresa (Informes de auditoría, reportes de incidentes, noticias de incidentes en la industria, etc.) se realiza una valoración de las vulnerabilidades para conocer la probabilidad de ocurrencia.	
4	Se realiza un análisis de impacto por activo en base a las amenazas y vulnerabilidades detectadas para cada uno de ellos de acuerdo a los 7 Principios de la seguridad de la Información además de su impacto financiero y de imagen.	
5	Conocidos la probabilidad de ocurrencia y el impacto ponderado de ocurrencia se calcula el riesgo inherente de cada activo respecto a sus vulnerabilidades y amenazas.	

Tabla 39: Lista de chequeo acciones Fase II

3. Fase III: Desarrollo de Controles y Mitigación de Riesgos

En este punto, ya conociendo los riesgos que corren los diferentes activos, se entran a analizar los controles existentes o que deben ser desarrollados por la organización para eliminar o minimizar la probabilidad de que una amenaza explote una vulnerabilidad del sistema y genere daños a la compañía. De este modo, por ejemplo, una vulnerabilidad tipo debilidad en el sistema o en un procedimiento, puede ser difícilmente explotada o su probabilidad es baja en la medida en que la fuente de amenaza tengo poco interés en ella o sea poco explotable, o bien haya un control efectivo que pueda reducir o eliminar esa probabilidad.

En esta nueva etapa se definen los procedimientos que la organización debe desarrollar y seguir para mitigar o eliminar los riesgos identificados. La finalidad de las recomendaciones de control es reducir el nivel de riesgo de los sistemas y activos a un nivel aceptable. Empecemos por algunos factores que vale la pena tener siempre en cuenta primero a la hora de empezar a definir los controles:

- Eficiencia de los controles ya existentes o que se encuentren disponibles o recomendados.
- La legislación nacional y las reglamentaciones.
- Las políticas organizacionales.
- El impacto operacional de introducir nuevos controles.
- La seguridad y la confiabilidad.

En el documento anexo de plantillas, en la sección 6, se encuentra la plantilla sugerida para el registro de los controles planeados para la mitigación de riesgos según la clasificación que se describirá a continuación.

3.1 Métodos de Control

Los controles de seguridad abarcan métodos técnicos y no técnicos. Los técnicos comprenden las salvaguardas incorporadas en infraestructura computacional de software y hardware e infraestructura física (sistemas de detección de intrusos, sensores biométricos, redes de cámaras, etc.) y los no técnicos son los controles de operación y administración (políticas de seguridad, procedimientos de operación, seguridad de personal, física y de entorno, etc.)

3.2 Categoría de Control

Al implementar controles para la mitigación de los riesgos, una organización debe considerar controles de seguridad *técnicos, de administración y operacionales*, o una combinación de ellos. Cuando estos controles son usados de forma apropiada pueden prevenir, limitar o eliminar el daño de una fuente de amenaza a la misión de la organización.
Los controles de seguridad técnicos, operacionales y de administración, tienen, entre otros, como constante los controles de prevención y de detección que se definen así: [3]

- **Controles de Prevención:** Estos inhiben intentos de violación de la seguridad y sus políticas e incluyen controles como el de acceso, autenticación, medidas de archivado, etc.
- **Controles de detección:** Estos alertan sobre violaciones a la seguridad o intenciones de violación de sus políticas y esquemas. Incluyen controles tales como la detección de intrusos, procedimientos de auditoria, etc.

3.2.1 Controles de seguridad técnicos

Este tipo de controles pueden ser utilizados para mitigar cierto tipo de amenazas que involucran usualmente arquitecturas de sistemas, disciplinas de ingenierías y paquetes de seguridad con una mezcla de software, hardware y firmware. Estos tres elementos deben acoplarse bien para asegurar información crítica, activos de información y sistemas completos.
Los controles técnicos se agrupan de la siguiente manera:

Controles de soporte: Son controles genéricos y subrayan las principales capacidades de los sistemas de información. Estos controles son la base y deben estar funcionando para poder implementar otros. Por su naturaleza de soporte estos controles están estrechamente relacionados con otros. Los Controles de Soporte son:

- **Identificación:** Este control provee la habilidad de identificar individualmente a usuarios, procesos y demás activos de información. Es importante que tanto sujetos como objetos estén identificados para poder implementar cualquier otro control.
- **Manejo de llaves:** El manejo de llaves debe ser manejado con cuidadosa seguridad en la medida en que es soporte de otros controles. La administración de llaves incluye su generación, distribución, almacenamiento y mantenimiento.
- **Administración de la seguridad:** Estos sistemas deben ser montados y configurados en coincidencia con las instalaciones específicas y sus áreas, y considerando sus cambios y particularidades operacionales.

Controles de prevención: Se concentran en primera instancia en prevenir que brechas de seguridad ocurran. Estos controles que pueden frenar intentos por violar las políticas de seguridad incluyen:

- **Autenticación:** El control de autenticación provee el mecanismo para identificar la identidad de un sujeto y asegurar que dicha identidad es válida. Estos mecanismos incluyen contraseñas, números de identificación personales, tokens y carnets, tarjetas inteligentes, certificados digitales y Kerberos.
- **Autorización:** El control de autorización permite la especificación y la subsiguiente administración de las acciones permitidas para un determinado sistema o grupo de activos.
- **Aplicación de controles de acceso:** La integridad y la confidencialidad de los activos está reforzada por los controles de acceso. Cuando un sujeto que solicita acceso ha sido autorizado a acceder a un determinado sector, activo o sistema, es importante hacer cumplir las políticas de seguridad. Estos controles basados en las políticas se imponen vía mecanismos de control de acceso distribuidos en los sistemas o a lo largo de las instalaciones.
- **No repudiación:** La rendición de cuentas de los sistemas de seguridad depende de su habilidad para asegurar que los usuarios no puedan negar sus acciones y comportamientos. La no repudiación abarca prevención y detección. Se sitúa en la categoría de prevención porque los mecanismos implementados previenen una repudiación exitosa. Esto pude aplicarse tanto para envíos y entregas, entradas y salidas, horas de acceso y utilización, etc.
- **Comunicaciones protegidas:** La habilidad para lograr una buena seguridad está fuertemente basada en la confiabilidad de las comunicaciones. Los controles para proteger las comunicaciones aseguran la integridad, disponibilidad y confidencialidad de la información crítica en su transmisión y tráfico. Las comunicaciones protegidas usan protocolos de encriptación tales como VPN, IPSEC, MD5, códigos y palabras en clave, etc. con el fin de minimizar las amenazas en cuanto a repetición, interceptación, intervención o modificación.

Controles de detección y recuperación: Estos controles se basan en la detección y la recuperación de brechas de seguridad. Estos controles alertan de violaciones o intentos de violaciones de las políticas de seguridad e incluyen guías de control y auditoría, y métodos de detección de intrusión. Los controles de recuperación sirven para restaurar los sistemas a estados anteriores a un evento adverso. Estos complementos son necesarios como un complemento a los controles de soporte y de prevención puesto que el riesgo de materialización de una amenaza nunca es cero, es decir, ningún control es perfecto. Estos controles incluyen:

- **Auditoría:** La auditoría de eventos relevantes de seguridad y el monitoreo y seguimiento de anormalidades en los sistemas son elementos clave en la detección después de, y la recuperación de brechas de seguridad.
- **Detección de intrusos y contención:** Es esencial detectar rechas de seguridad para poder darles respuesta en un tiempo apropiado. Es de poca utilidad detectar una brecha si no pueden tomarse medidas en respuesta. La respuesta es la contención.
- **Pruebas de integridad:** Los controles de pruebas de integridad analizan la integridad e irregularidades de los sistemas y activos e identifican potenciales amenazas. Estos controles no previenen violaciones a las políticas de seguridad pero las detectan y ayudan a determinar las medidas de corrección necesarias.
- **Retorno a estados seguros:** Estos mecanismos permiten a los sistemas volver a un estado, que se sabe seguro, luego de que se presenta una brecha en la seguridad:

3.2.2 Controles de administración de seguridad

Los controles de administración de seguridad, en conjunción con los controles técnicos y los operacionales, se implementan para manejar y reducir el riesgo de pérdida y proteger la misión de la organización. Los controles de administración se centran en estipular las políticas, guías y estándares de protección de los activos de información, que son llevados a cabo por procedimientos operacionales para satisfacer las metas y misiones de la organización.
Los controles de administración de seguridad se agrupan de la siguiente manera:

Controles de prevención: Que incluyen:

- Asignar responsabilidades de seguridad para para cerciorar la adecuada seguridad en los sistemas críticos.
- Desarrollar y mantener planes de seguridad para documentar controles y direccionar planes en pro del mantenimiento de la misión de la organización.
- Implementar controles de seguridad de personal incluyendo separación de responsabilidades, privilegios mínimos y normas de acceso y uso de activos.
- Coordinar los entrenamientos técnicos y de seguridad en el uso de activos y sistemas de modo tal que los usuarios tengan claras cuáles son sus responsabilidades respecto al buen uso y buenas prácticas de seguridad que protejan la misión de la organización.

Controles de detección: Que incluyen:

- Implementar controles de seguridad de personal incluyendo acreditación de personal, rotación de deberes e investigaciones de antecedentes.
- Realizar revisiones periódicas de los controles de seguridad para cerciorar su efectividad.
- Hacer auditorías internas periódicas.
- Poner en marcha un proceso de administración de riesgos para evaluar y mitigar los riesgos.
- Autorizar a los sistemas, usuarios y administradores a aceptar el riesgo residual y trabajar con él.

Controles de recuperación: Que incluyen:

- Proveer continuidad en soporte y desarrollo, pruebas y mantenimiento de los planes operativos para asegurar la recuperación del negocio y la continuación de las operaciones en las emergencias o desastres.
- Establecer una capacidad de respuesta a incidentes que prepare a la organización para reconocer, reportar y responder a un incidente y retornar al negocio a un buen estado de operación.

3.2.3 Controles de seguridad operativos

Los estándares de seguridad de una organización deben establecer un conjunto de controles y guías para asegurar y definir buenos procesos de seguridad que hagan buen uso de los activos y recursos de la organización enfocándolos acorde a las metas y misión. La administración juega un rol vital observando la implantación de políticas y asegurando el apropiado establecimiento de controles de operación apropiados.

Los controles operativos, implementados de acuerdo a un set de requerimientos base y buenas prácticas industriales, sirven para corregir deficiencias operacionales que pueden ser explotadas como vulnerabilidades por potenciales fuentes de amenaza. Para asegurar consistencia y uniformidad en estas operaciones, deben definirse con claridad procedimientos paso a paso y métodos para su implementación, además de ser documentados y monitoreados.

Los controles de seguridad operacional se agrupan de la siguiente manera:

Controles de prevención: Que incluyen entre otros:

- Controles de acceso a medios y disposición como controles de acceso físico, eliminación de estática, desmagnetización, etc.
- Limitar la distribución externa de información.
- Control de malware.
- Salvaguardar las instalaciones, por ejemplo con guardias de seguridad, procedimiento de registro de visitantes, sistemas de tarjetas electrónicas, controles de acceso biométrico, administración y distribución de llaves y candados, barreras perimetrales, etc.
- Asegurar los conductos de cables.
- Procurar backups, como procedimientos de backup de información y sistemas, logs de transacciones en bases de datos que ayuden a la recuperación de estados anteriores, etc.
- Establecer procedimientos y normas para el almacenamiento externo de la información de la organización; en dispositivos externos a los de propiedad de la empresa y los que están fuera de límites de sus instalaciones.
- Crear políticas y campañas de autocuidado en los empleados con sus espacios de trabajo, equipos portátiles, móviles, etc.
- Crear controles contra incendios, humedad, cambios de temperatura, etc.
- Asegurar el buen abastecimiento de energía eléctrica y sus fuentes de reserva en caso de fallos.

Controles de detección: que incluyen entre otros:

- Proveer seguridad física como sistemas de detección de movimientos, sistemas cerrados de televisión y vigilancia por cámaras, sensores y alarmas, etc.
- Asegurar el entorno con detectores de humo y fuego, sensores y alarmas, etc.

3.3 Análisis de círculos concéntricos de seguridad física

Para definir controles que implementen y maximicen la seguridad física es importante, además de tener un buen levantamiento de activos, conocer muy bien el entorno espacial en que se encuentras estos dado que en seguridad física es este entorno sobre el que, en últimas, deberán enfocarse los

esfuerzos de aseguramiento para mantener la integridad, la confidencialidad y la disponibilidad de los activos de información. De este modo debe hacerse un análisis de afuera a adentro del entorno que circunda al activo o conjunto de activos que deseamos proteger para ir escalando en niveles de mayor a menor abstracción del entorno y su seguridad física.
Esta perspectiva de la seguridad física es llamada de Círculos Concéntricos de seguridad y analizan las condiciones de entorno de seguridad de la organización de afuera hacia adentro de esta manera: [8]

3.3.1 El vecindario

Conocer el vecindario en que se alojan las instalaciones de la organización es clave para empezar a armar un plan y controles de seguridad. Estudiar este entorno implica enfocarse en conocer la situación social, política, económica y de seguridad de la zona. Identificar allí a los actores sociales y por medio de ellos conocer la situación de seguridad y delincuencia de la zona así como establecer relaciones cordiales y armoniosas que resulten beneficiosas para toda la comunidad y grupos sociales y empresariales de la zona.

3.3.2 La barrera perimetral

Esta representa la seguridad externa y tiene como objeto disuadir la entrada, retardarla o detenerla según sus cualidades de resistencia, consistencia o por la dificultad o el riesgo que implique intentar un traspaso. Además ayuda a detectar un intento de traspaso con la ayuda de algún tipo de señal y con ello ubicar el punto exacto donde se ejecuta la intrusión. En caso de materializarse la intrusión debe lanzar una alerta al siguiente círculo.

Estas barreras perimetrales pueden ser naturales (como un rio, una zanja, una pendiente) o estructurales (como un muro, una reja, una malla), y deben reforzarse y ser cuidadas. Sin un refuerzo adecuado como iluminación, alambrado de pues, una reja resistente, y sin un cuidado riguroso como guardias, alarmas, detectores de movimiento, perros, mecanismos de refuerzo para evitar su deterioro, etc. la barreras perimetrales no son una protección fiable.

Las barreras para poder garantizar una buena seguridad deben ser vigiladas y patrulladas constantemente además de permanecer limpias para permitir una visual clara. Elementos como maleza, residuos u obstáculos deben retirarse para que no puedan servir de escondite a un posible

intruso. Así mismo la barrera debe encontrarse sobre un plano evitando depresiones, y su línea debe ser recta, sin ángulos pronunciados, recovecos, o estructuras laberínticas.
Entre la barrera perimetral y las instalaciones se debe procurar un área libre para la zona de seguridad dentro de la barrera. En caso de no contarse con mucho espacio, se debe aumentar el tamaño de la barrera y reforzarla con equipos de detección y dificultad de traspaso.

Las barreras son perímetros defensivos, y una vez establecidos deben ser inspeccionados periódicamente. El equipo de vigilancia debe cerciorarse de la resistencia de las puertas, probar las cerraduras, mirar la integridad de las mallas que no deben tener agujeros, los muros no deben tener baches ni grietas que permitan el escalamiento y deben buscarse signos de escalamiento, las erosiones deben corregirse y los sistemas electrónicos estar siempre actualizados y probados.

Hay un elemento adicional que debe partir en la zona de la barrera perimetral y debe continuar protagonista en todas las instalaciones de la organización de allí hacia adentro: La iluminación de protección. La iluminación es en primera instancia un disuasorio para los intrusos, por lo que debe cubrir las áreas de riesgo y de posible intrusión evitando visibilizar los puestos de los guardas. Los haces de luz no pueden incomodar a los vecinos, los tránsitos vehiculares o peatonales; y en caso de fallar una, los conos de luz deben traslaparse para que no queden zonas sin cubrimiento de luz.
El sistema de iluminación debe ser fácil de mantener y de operar, debe estar protegida contra ataques y tener siempre un respaldo de energía eléctrica en caso de cese del servicio.

3.3.3 Áreas intermedias abiertas

Las áreas abiertas intermedias son aquellas que se ubican entre las barreras perimetrales y los muros de periféricos de la organización. En estas áreas suelen ubicarse las zonas de parqueaderos, de despachos y recibos de mercancías, zonas verdes, etc. Estas áreas son la segunda línea de defensa pero tiene la particularidad de ser fácilmente observable desde fuera de las barreras perimetrales.
En algunos casos estas zonas son utilizadas para el almacenamiento o apilamiento provisional de materiales, insumos, chatarra, basuras y demás, que exigen ser almacenados de manera ordenada y planeada para evitar que se conviertan en posibles escondites de intrusos.

3.3.4 Muros periféricos de las instalaciones

Esta tercera barrera de protección corresponde a los muros y estructuras fachada de los edificios de la organización Estos son la barrera que da acceso directo a las áreas internas de la organización; cualquier bache de seguridad en ellas daría importantes accesos y beneficios a un intruso,
El material más usual usado para levantar estos muros es desde luego el ladrillo en combinación con otros materiales estructurales; y los accesos de luz, ventilación y personal suelen ser puertas metálicas o de vidrio, persianas metálicas, rejas, y mallas. El tamaño de estas ventanas o ventilaciones debe ser menor al del tamaño promedio de las mercancías importantes y los activos valiosos para asegurar que empleados deshonestos los saque por allí y los recojan a la salida.
En edificaciones donde el factor estético es importante como torres de oficinas, apartamentos, etc. y no permiten el uso de rejas o mallas, el uso de vidrio de seguridad es recomendado, a pesar de su alto costo por ser resistente a golpes y no da muestras de envejecimiento ni desgaste.

3.3.5 Áreas internas de los edificios

Las áreas internas del edificio son las áreas dentro de los muros periféricos de las instalaciones. Representan la mayor parte de las áreas de trabajo. Para determinar el grado de seguridad de estas áreas es importante conocer bien la importancia de las personas que laboran en ellas, el tipo de operaciones que ejecutan y los activos e información que utilizan en dichas labores.

Un primer elemento a analizar para la seguridad física de las área internas son los puntos de acceso. Respecto a las puertas es importante examinar cada una de acuerdo al grado de seguridad requerido para cada una de las dependencias a las que dan acceso. El tipo de operación realizada en cada dependencia determinará su importancia y por ello el tipo de puerta, cerradura y llave a utilizar.

Frente a la estructura de las puertas, hay que procurar unas de estructura fuerte y pesada para zonas de procesos e información crítica. Su cerradura debe ser resistente y confiable, su marco preferiblemente metálico y sus bisagras no deben quedar a la vista ya que podrían ser fácilmente removidas por un intruso.

La decisión frente al tipo de puerta y sus características debe hacerse de acuerdo a un patrón de tráfico y la importancia de éste. Muchas restricciones para mucho tráfico también es contraproducente. Para las áreas restringidas como el centro de cómputo, oficinas de investigación y desarrollo, y otras administrativas e importantes deberían contar con cierres automáticos y controles personalizados de acceso.

Frente al movimiento en las áreas internas sus controles incluyen:

- ✓ **Control de accesos e identificación de personal:**

  Un principio rector es que todo usuario debe registrarse a la entrada o a la salida. Para esto la organización puede apoyarse en sistemas electrónicos. Estos sistemas pueden complementarse con sistemas cerrados de televisión que apoyen el seguimiento a los usuarios, el movimiento en las diferentes áreas y la identificación de intrusos.

  Para el control de visitantes es recomendable implementar un sistema de asignación de citas y sus visitas deben basarse en trámites cortos. Al ingreso se debe hacer el registro de datos de entrada y asignar una credencial de visitante acompañada de una indicación de rutas claras de entrada y salida para evitar el merodeo y el extravío. Tras esto el personal de recepción debe hacerse cargo del visitante y hacerlo esperar en un lugar especialmente dispuesto para ellos. El visitante debe permanecer allí hasta ser atendido por la persona solicitada por el y ser conducido a su oficina o estación de trabajo. Al momento de la salida el personal de seguridad debe solicitar la credencial de vuelta y registrar la hora de salida.

  En lo que respecta a los empleados, no se requiere un sistema muy sofisticado de identificación de personal en organizaciones con menos de 50 empleados ya que el personal de seguridad puede conocer con facilidad a cada empleado personalmente. Cuando la cantidad de empleados es superior o hay un sistema de turnos que rotan es importante identificar a los empleados tanto a su ingreso como en su permanencia en las instalaciones. Las identificaciones más usuales son carnets con fotografía, nombre completo del empleado, cargo, área de la organización, y la firma de quien expide la credencial.

- ✓ **Orientación e información en el interior:**

  Suele ser común que algunos visitantes o empleados nuevos lleguen a una organización con un considerable tamaño y no sepan orientarse adecuadamente ignorando donde está y qué ruta debe tomar para la dependencia a la que se dirige. Para mitigar este inconveniente debe disponerse de un adecuado sistema de señalización de áreas y oficinas. De acuerdo a requerimientos de ley también deben resaltarse las salidas de emergencia y verse los mapas

con las rutas de evacuación. Estos mapas son croquis de las instalaciones que ayudan a la orientación y debe colocarse en las esquinas de los edificios. En la entrada de cada oficina debe haber un aviso con el área a la que pertenece la oficina y el cargo de quien la ocupa. Puede o no añadirse también el nombre de quien la ocupa.

- ✓ **Control de paquetes:**

Respecto al ingreso y extracción de paquetes para los visitantes, debe plantearse un sistema de verificación de contenido. Solicitar a los visitantes presentar a la entrada y salida sus bolsos abiertos y en caso de portar equipos móviles o portátiles como laptops, tabletas, cámaras fotográficas, u otros equipos que también puedan hacer parte de los activos de la organización, declararlo en la portería y registrar su ingreso y salida.

- ✓ **Control e identificación de vehículos**

Es muy fácil esconder equipos y mercancías sustraídas en un vehículo y encontrarlas resulta complicado en procedimiento y permisos. Por lo tanto los esfuerzos se deben enfocar en las debilidades que facilitan un hurto que son: la proximidad entre los activos sustraíbles y el vehículo, y poca o inoperante vigilancia que crea una oportunidad y una brecha de tiempo considerable para ejecutar el ilícito. Para evitar esto los controles propuestos son, en primera instancia que la zona de parqueadero se encuentre en las áreas abiertas intermedias entre las instalaciones y las barreras periféricas, además de estar separadas las zonas de recibo y de embarque. El tiempo de entrada, salida yd e procesos debe ser el menor posible y debe evitarse dejar activos expuestos siempre manteniendo una vigilancia activa.

3.4 Análisis para la seguridad física sobre Instalaciones o edificios.

Al ser el edificio el que alberga a la organización y sus activos, debe ser el primero en ser estudiado, no solo por esta cualidad sino por ser también el activo más problemático, puesto que constituye en entorno ya diseñado y construido, no modificable y que suele tener un uso compartido de muchos sistemas humanos y tecnológicos; de este modo cualquier modificación en pro de la seguridad incurre en un gasto económico importante el cual debe ser evaluado cuidadosamente en un análisis de costo-beneficio con los riesgos de seguridad y sus impactos.

Dentro del análisis de los edificios es importante conocer bien su estructura: Estudiar sus planos para entender el reparto de las áreas, los accesos, los sistemas de seguridad, el suministro eléctrico, conductos de gas y agua, sistemas contra incendios, salidas de emergencia, etc. Puede haber áreas de mayor incidencia de terremotos o desplazamientos y deben existir sistemas de protección también contra estos problemas. La ayuda de un profesional puede ser de gran ayuda en este estudio.
Aquí reposan las recomendaciones de control de seguridad para los tipos de activos de información: instalaciones, personal, información de funcionamiento y activos esenciales según lo descrito en la sección 5.3.1. [9]

3.4.1 El suministro eléctrico

El estudio sobre el suministro de energía debe enfocarse sobre los sistemas de suministro a los sistemas que queremos proteger y que tienen especial relevancia para el negocio más que en el suministro de energía para el personal y zonas comunes. No representa, por ejemplo, la misma criticidad el sistema de refrigeración del centro de cómputo que el aire acondicionado de las oficinas.
El suministro eléctrico suele estar dividido en 2 etapas: Una externa que es la infraestructura proveída como servicio por la empresa de energía eléctrica, cuyo límite con la organización es el punto de conexión con el sistema de tarificación. La segunda etapa corresponde a los sistemas internos de suministro. Frente a la primera etapa, sus dispositivos, cualidades y mantenimiento no es responsabilidad de la organización y cualquier riesgo se transfiere a la empresa de suministro de energía en calidad de prestador del servicio. Lo que sí debe tomarse en cuenta son los sistemas y mecanismos de redundancia con los que cuente dicha empresa. Esta información se consigue en servicio al cliente y es importante para un análisis de riesgos y determinación de controles en cuanto esta redundancia pueda alterar los planes de seguridad. En caso de sistemas críticos la redundancia puede ser contratada como servicio adicional en caso de que la empresa cuente con él. Caso contrario la responsabilidad pasa a la organización y pueden utilizarse sistemas de respaldo como generadores eléctricos que funcionan con combustible y pueden asegurar el flujo eléctrico por un largo período de tiempo en caso de una interrupción. De nuevo su costo de compra, mantenimiento y uso debe estar supeditado a la criticidad de los sistemas a los que provee.

Una cuestión importante a comprobar es la posibilidad de que una fuente de amenaza, probablemente un intruso malintencionado quiera cortar el suministro. Para esto debe comprobarse

que no sea fácil el acceso a los sistemas proveedores o la caja de conexiones. Es imprescindible comprobar que se cumplen las necesidades de protección para todas as instalaciones y cada una de sus zonas, de modo que ante un fallo puedan aislarse del problema en la mayor medida posible. Por último todos los dispositivos deben estar homologados y las instalaciones deben cumplir con la reglamentación de baja tensión. Esto proporciona protección sobre equipos defectuosos.

3.4.2 Accesos físicos a las instalaciones

Tras haber analizado los diferentes accesos y barreras con los que cuentan las instalaciones de la organización en la sección anterior, hay que tener en cuenta que los edificios tienen accesos obvios y otros no tan obvios que pueden ser utilizados por intrusos: Los obvios son las puertas y ventanas que dan hacia las zonas abiertas o hacia el vecindario, y los no obvios los accesos a la ventilación, los techos, las claraboyas, los accesos de mantenimiento o de servicio y las alcantarillas.

Un intensivo estudio de los accesos a las instalaciones es fundamental para la seguridad física. Los intrusos suelen contar con tiempo y paciencia y por más sistemas de seguridad que haya desplegados, una brecha en los accesos es gravísima: Un intruso adentro puede maniobrar y tener más accesos que desde fuera. En la medida de lo posible la instalación de rejillas de seguridad en las rejillas y puertas y ventanas de seguridad en entradas secundarias o instrumentos de autenticación pueden ayudar a mitigar riesgos. En caso contrario es recomendable un equipo de personal de vigilancia de tiempo completo que impida cualquier intrusión. Como siempre el nivel de protección debe ser proporcional al nivel de criticidad de los sistemas y activos de información a resguardar.

Las medidas de seguridad pueden variar según la variación horaria del trabajo en la organización: Para las horas laborales es aconsejable el control de acceso a personal con tarjetas de identificación y registros de entrada y salida. Para los horarios de inactividad, en cambio, los sistemas de vigilancia por con cámaras de seguridad y de detección de movimiento deben estar más alerta y el enfoque debe estar en los accesos secundarios.
Por medio de un especialista o personal entrenado de la organización pueden hacerse algunas pruebas de intrusión para evaluar la efectividad de los sistemas. Hay abundante conocimiento sobre evasión de cámaras y forzamiento de cerraduras o lock picking.

3.4.3 Controles contra incendios e incidentes

Los sistemas contra incendios y otros desastres son difíciles de instalar posterior a la construcción del edificio ya que suelen ser instalados en ese proceso. Los sistemas de control contra incendios involucran sistemas de detección de humo y de sofocamiento de llamas. Estos últimos suelen utilizar químicos de extinción, no agua que es enemiga de los equipos hardware y demás activos.

Sistemas de monitoreo de humedad, temperatura e incluso de líquidos pueden ser necesarios. En caso de una ruptura de tuberías, una inundación podría ser sumamente destructiva. Como siempre, un esquema de vigilancia y continuo mantenimiento de estructuras aportan más en materia de prevención que en mitigación.

La seguridad del personal es igualmente vital para la organización y dentro de los estudios de seguridad deben contemplarse los planes de evacuación y atención de emergencias en caso de incendios, terremotos, amenazas estructurales, etc. estos planes deben ser revisados periódicamente para constatar su valides y utilidad.

3.4.4 Control de warchalking

En el mundo del hacking o piratería informática el Warchalking es el marcado de instalaciones por medio de grafitis o tizas para indicar a los ojos que sepan reconocer los que en esa edificación hay vulnerabilidades de acceso a redes inalámbricas o datos. Un hacker podría tratar de tener acceso a la red interna obteniendo una IP válida por medio del servidor DHCP con un equipo portátil con conexión wireless. Periódicamente deben inspeccionarse las fachadas de las instalaciones en busca de signos de warchalking u otras marcas sospechosas ya que la amenaza se expande a innumerables atacantes que pueden reconocer las señales exponiendo gravemente a la red de la empresa. La simbología del warchalking cambia con el tiempo y de acuerdo a las diferentes escuelas de hackers, por lo cual se debe sospechar de cualquier tipo de marca asumiendo que la vulnerabilidad de seguridad no es únicamente física sino lógica y se deben reforzar los controles en los dos ámbitos.

3.5 Análisis para la seguridad física sobre el entorno de los activos de información y la seguridad física sobre los activos de información

El entorno físico del hardware se define como el entorno donde se sitúan el hardware, los dispositivos de red y los centros de cómputo. Estudiar su seguridad supone el estudio de la localización del hardware, el acceso físico del personal a estos ambientes, todo el cableado que lo interconecta o que lo alimenta con energía, los controles de temperatura, humedad y demás condiciones de clima, el montaje sobre el que se instala y los métodos de administración y gestión de dichos recursos de hardware,
Respecto a la seguridad de los activos, esta sección se refiere a los activos hardware, redes de comunicación, soportes de información, servicios y equipos auxiliares descritos en la sección 1.1.

Estos activos suelen estar más cercanos a los usuarios lo que torna más arduo su aseguramiento ya que están más expuestos a mayores peligros de mal uso o uso malintencionado. Esto obliga a que las configuraciones tanto a nivel físico como lógico propendan a dificultar más la labor de vulnerar estos activos, ya que se debe hacer el análisis sobre la base de que el personal no sigue a cabalidad las normas o que intrusos ya han podido vulnerar los sistemas de acceso y ahora pueden manipular estos activos.
Este estudio se divide en 6 tipos de entornos con el fin de hacer un análisis más profundo y puntual sobre la seguridad física de los activos antes mencionados.

3.5.1 Procedimientos de control para centros de cómputo

Establecer controles para la seguridad física de los centros de cómputo es una labor prioritaria dentro de los planes de seguridad. La complejidad de esta labor depende de las particularidades de los centros de cómputo, incluyendo la cantidad de espacio que ocupen en la organización y la masividad y complejidad de sus estructuras. A continuación se presentan las cuestiones clave sobre las que se debe reflexionar a la hora de determinar controles sobre los centros de cómputo: [7]

- ✓ En caso de que el centro de cómputo ocupe toda una edificación el plan de seguridad debe direccionarse de acuerdo a todos los círculos periféricos anteriormente descritos.
- ✓ En caso de que el centro de cómputo ocupe únicamente una parte de la edificación el plan de seguridad debe direccionarse a cada área interna donde se encuentre.
- ✓ El control de acceso y de administración son fundamentales en un plan de seguridad de centros de cómputo que debe indicar quién tiene acceso, cómo se garantiza ese acceso, cómo se maneja el acceso de visitantes y proveedores, y cómo lidiar con brechas en las políticas de seguridad.

- ✓ ¿Cada cuánto tiempo deben revisarse los registros de acceso?
- ✓ ¿Cuáles son los procedimientos para asegurar los equipos, sistemas de cableado, equipos de encriptación, y contenedores de almacenamiento definidos como más sensibles?
- ✓ El listado de métodos de seguridad para los equipos auxiliares incluyendo aires acondicionados, soportes de energía, conexiones de red, y sistemas de alimentación de emergencia.
- ✓ Lista de procedimientos de seguridad para las horas de operación, horas de no operación y operación de emergencia
- ✓ ¿Cómo se actualizan los logs de registro de todos los equipos utilizados incluyendo información de configuración y números seriales?
- ✓ ¿Cómo se actualizan las listas de personal autorizado a acceder a áreas privilegiadas?
- ✓ ¿Cómo son mantenidos los equipos y las condiciones ambientales?
- ✓ ¿Cómo y cuándo son inspeccionados los paquetes que entran y salen del centro de cómputo?

Acceso: Los centros de cómputo suelen tener los equipos más costosos (al menos en el entorno de IT) y manejan la información e infraestructura más sensible, lo que exige que su seguridad sea especialmente óptima. Su sistema de acceso debe ser suficientemente seguro preferiblemente con una puerta blindada y en lo posible con personal de vigilancia que compruebe el acceso por medio de tarjetas de identificación o sistemas de identificación biométrica.

Conectividad: Como se describió anteriormente, el suministro eléctrico debe estar asegurado de forma redundante y aislado de las otras zonas del edificio. El sistema de conexión a la red corporativa debe estar asegurado mediante varias conexiones redundantes que permitan que una falle y el servicio siga activo. Esta conexión redundante a fallos también aplica para conexiones a redes públicas.

Ambiente e incidentes: El sistema de aire acondicionado es imprescindible si se tiene una cantidad considerable de hardware dentro del centro. Es aconsejable tener un sistema de monitoreo de humedad y temperatura para poder asegurar niveles óptimos de funcionamiento. Es imprescindible igualmente un sistema de detección de incendios que permita alertar al personal para que proceda a apagarlo manualmente con extintores dispuestos en el centro, o que lo extinga automáticamente por medio de canales de conducción de químicos de extinción. Es aconsejable que los armarios y racks sean de materiales ignífugos.

Backups: Frente a los backups de información es aconsejable que los servidores que los almacenen se encuentren en salas, e incluso, en edificios diferentes para mitigar riesgos sobre incidentes propios del centro de cómputo. Una opción alternativa y muy utilizada es la contratación de servicios de backup que tienen toda la infraestructura especializada para el almacenamiento de información en cintas magnéticas en las mejores condiciones de seguridad. Empresas que prestan estos servicios recogen periódicamente las cintas y disponen de su custodia de acuerdo a los requerimientos del cliente.

Redundancia: Una buena forma de mejorar la seguridad física y asegurar la integridad y la disponibilidad de la información es mantener servidores y copias de la información redundantes sincronizados en diferentes localizaciones. Es necesario contar con suficiente ancho de banda para interconectar estos sistemas corporativos. Los sistemas de gestión y de servidores comerciales distribuidos son costosos, pero es posible implementar soluciones sobre software libre a un buen precio y con buenas facilidades de mantenimiento. Es importante que la redundancia también se aplique a los sistemas de interconexión para asegurar los enlaces de comunicación, sobre todo cuando se trata de datos y procesos críticos. Es imprescindible hacer un estudio de seguridad física para todas las instalaciones que alberguen los sistemas distribuidos.

Montaje: Pueden presentarse problemas de seguridad cuando no hemos previsto el espacio total y el tamaño de los armarios que se requieren para instalar todos los equipos: Es importante sobredimensionar dichas áreas y espacios para evitar faltantes o imprevisiones de crecimiento. Usualmente los armarios y racks suelen venir con cerradoras no muy complejas que un intruso experto podría fácilmente vulnerar con técnicas de lock picking que se encuentran sin problemas por internet; por ello es indispensable no sólo conformarse con los armarios sino revisar, y de ser necesario, reforzar sus cerraduras. De cualquier modo no hay que olvidar la seguridad propia de los equipos de red dentro de los armarios; aún con buenas cerraduras la seguridad debe reforzarse informáticamente en las configuraciones propias de los equipos y sus BIOS para evitar cambios en el cableado, conexiones no permitidas, sniffers, cambios de configuraciones, etc.

3.5.1.1 Diseño óptimo de Centros de cómputo

La norma ANSI/TIA 942[10] define los lineamientos para la construcción óptima de centros de cómputo en cuanto a:

- **Diseño de cableado:** Aquí la norma presenta la guía para la planeación, el diseño y la instalación del cableado de un Centro de cómputo según los últimos estándares en la materia. Da lineamientos sobre:
    - El rendimiento del cobre y del cable de fibra
    - Los cables, conectores y el hardware de distribución
    - Las distancias en el cableado (Pisos elevados y cableado elevado)
    - La gestión del espacio

- **Diseño de instalaciones:**Aquí la norma presenta la guía para el diseño del centro de cómputo en los siguientes aspectos:
    - El tamaño del Centro de datos
    - La metodología de distribución de la energía
    - Las rutas, pasillos y espacios
    - Administración, operación y seguridad
    - La flexibilidad, la escalabilidad, la fiabilidad y la administración del espacio

- **Diseño de redes:** Aquí la norma presenta la guía para el diseño e implementación de las redes según los últimos estándares enfocándose en:
    - Soporte de sistemas heredados
    - Habilitar el despliegue rápido y eficiente de tecnologías nuevas y emergentes

Adicionalmente la norma ANSI/TIA 942 presenta anexos para profundizar n buenas prácticas en [11]:

- Consideraciones del diseño de cableado
- Administración de infraestructura de telecomunicaciones
- Información de acceso
- Coordinación de planes de equipo con otros ingenieros
- Consideraciones del espacio en los centros de cómputo
- La selección del sitio para el centro de cómputo

La norma ANSI/TIA 942 define 4 Niveles de desarrollo de centros de cómputo. Es recomendable estudiar estos niveles para definir cuál de ellos podría ser el apropiado según el negocio de la organización, sus necesidades y presupuesto. Los 4 niveles son [12]:

- Nivel I: Básico:
  - ✓ Es un centro con tutas únicas
  - ✓ No tiene componentes redundantes

- Nivel II: Componentes redundantes:
  - ✓ Es un centro con rutas únicas
  - ✓ Tiene componentes redundantes

- Nivel III: Un centro que permite hace mantenimiento sin interrupciones:
  - ✓ Sistemas multimódulos
  - ✓ Doble ruta de alimentación de potencia
  - ✓ Se pierde la redundancia en un fallo o durante el mantenimiento
  - ✓ Tiene ruta duales o múltiples

- Nivel IV: Centro tolerante a fallos:
  - ✓ Tiene componentes redundantes
  - ✓ Tiene fuente dual de potencia crítica garantizada
  - ✓ No hay pérdida de redundancia en presencia de un fallo simple o en caso de mantenimiento
  - ✓ Tiene rutas múltiples

La utilización y seguimiento de estándares puede, en las etapas de diseño e implementación, incluir directa e indirectamente pautas de seguridad física apropiadas y actualizadas. Una guía en español para esta labor, basada en la norma ANSI/TIA 942, es la Norma Técnica "Como diseñar un centro de Datos óptimo" de ADC Telecommunications Inc. [13] Disponible en http://ecaths1.s3.amazonaws.com/auditoriainformatica/1167828372.Norma_ANSI_EIA_TIA_942.pdf

3.5.1.2 Plan de protección contra el fuego

Un programa integral de protección contra el fuego define 4 etapas: [12]

- **Prevención:** Es la primera etapa y define las siguientes actividades:
  - ✓ Definir un Nivel de centro de cómputo según lo descrito en la sección anterior.

- ✓ Realizar el proceso de gestión de riesgos sobre el centro de cómputo según la Fase II de la presente guía.
- ✓ Crear un plan de emergencia contra el fuego el cual incluya:
  - Una brigada contra incendios
  - Una buena señalización de rutas de evacuación y salidas de emergencia
  - Una capacitación a los operadores y empleados en general
  - La implementación de un sistema de iluminación de emergencia
- ✓ De ser viable, diseñar un sistema de protección contra descargas atmosféricas y de protección contra sobretensiones eléctricas
- ✓ Realizar auditorías anuales de infraestructura

❖ **Detección:** La norma NFPA 76 [14] define los procedimientos y buenas prácticas estándar para la etapa de detección de incendios y señala los equipos de detección y su implementación en un sistema. Entre los equipos de detección destaca:

- Detectores EWFD: Detectores de incendio de alerta temprana, que son sistemas que usan humo, calor elevado o llamas para dar una alerta temprana de incendio.
- Detectores VEWFD: Detectores de amenaza muy temprana, que son los sistemas que detectan fuego de muy baja energía antes de que represente un peligro para las instalaciones.

❖ **Extinsión:** La norma NFPA 76 también brinda directrices sobre los sistemas de extinsión clasificándolos en:

- Sistemas con regaderas automáticas (Sprinklers)
- Sistemas con agentes gaseosos limpios (CO”, Halon, Inergen, FM-200, etc)
- Extintores manuales

Así mismo describe la forma de diseñar e instalar la red de sistemas de extinsión y de detección/extinsión dentro de un centro de cómputo.

❖ **Contención:** Aquí la norma detalla las características que debe tener una construcción resistente al fuego, que es una en la que las columnas, vigas, paredes, pisos y demás miembros estructurales tienen un tiempo de resistencia al fuego no menor a sus especificaciones.

La norma señala que los centros de cómputo deben estar separados de otras áreas del edificio por construcciones resistentes al fuego de no menos de una hora. En ellas, cada abertura que exista debe ser protegida para prevenir que el fuego se propague y restriñir el movimiento del humo de lado a lado del edificio.

En la sección de ESTÁNDARES Y NORMAS RECOMENDADAS se encuentran listadas más normas que pueden ser de gran ayuda para elaborar el plan de seguridad de los centros de cómputo desde su etapa de diseño y construcción.

3.5.2 Procedimientos de control para conexiones y cableado

Las conexiones y el cableado, especialmente los que se encuentran fuera del centro de cómputo necesitan ser asegurados para protegerlos de accesos no autorizados que violen potencialmente la integridad, la confidencialidad y la autorización. Esto previene interceptaciones, daño intencional, y daño accidental durante el mantenimiento. Sólo personal calificado y autorizado debe tener acceso a las áreas y conductos donde se concentran los cables y conexiones y debe evitarse que el cableado comparta conductos con otros sistemas como los de ventilación, plomería o calefacción. Las consideraciones sobre el proceso de aseguramiento de las conexiones y el cableado se describen a continuación: [7]

- ✓ ¿Cómo está controlado y monitoreado el acceso al cableado y las conexiones?
- ✓ ¿Qué tipo de puertas y cerraduras se utilizan para asegurar el cableado y las conexiones?
- ✓ ¿Qué tipo de alarmas o sistemas de monitoreo son utilizados para controlar el acceso al cableado y las conexiones?
- ✓ ¿Cómo son monitoreados los proveedores de servicio cuando y si necesitan acceso a las áreas de cableado y conexiones?
- ✓ ¿Cómo se mantienen los logs de registro de acceso a las área de cableado y conexiones?
- ✓ ¿Cómo se controlan las llaves o los códigos de acceso a las áreas de cableado y conexiones?
- ✓ ¿Cómo se transmiten las señales sobre cableado y conexiones protegidas contra intercepciones?

Interconexión: Aquí el foco se posa sobre la arquitectura de la red en el edificio y no en los dispositivos. Una red típica consta de un par de enrutadores que permiten la conectividad con el exterior (usualmente una red troncal Gigabit Ethernet) que se extiende por todas las instalaciones, y concentradores que distribuyen el tráfico por la red interna. Buscar puntos de fallo puede ayudar a prevenir caídas de la red mientras se implementen conexiones redundantes. Es importante también estudiar los circuitos de cableado que recorren las instalaciones y cómo han sido entubados y

distribuidos. Su entubamiento debe tener suficiente rigidez para limitar seccionamientos o cortes malintencionados. Para redes de fibra óptica realizar pruebas periódicas de velocidad conexión permiten conocer el estado de las redes y sus posibles puntos de fallo de acuerdo a los resultados de conexión por zonas. Frente a los routers y switches deben procurarse conexiones redundantes y condiciones de seguridad no hostiles para garantizar una conexión permanente entre departamentos, y entre el exterior y la empresa.

Cableado eléctrico: Se deben cumplir los requerimientos mínimos sobre tensión de acuerdo a las normas vigente. Hay que buscar posibles fallos en enchufes y toma corrientes que puedan provocar chispas. Un asesoramiento con el electricista dará las pautas sobre densidad y diámetro del cableado para obtener el mejor beneficio calculando la potencia máxima que consumirán los equipos de la organización; este cálculo siempre debe sobreestimarse para prever posibles nuevos dispositivos. Un factor adicional es que el cableado en alta concentración debe estar en un lugar alejado de equipos de cómputo para evitar problemas eléctricos por exposición a campos magnéticos generados por las altas corrientes.

Cableado de telefonía: Aquí las precauciones no son más que las esenciales: Mantenerlo lejos del cableado eléctrico, cumplir con los estándares y normativas vigentes, buscar un ambiente seguro que evite cortes o interferencia de usuarios maliciosos. Por demás este cableado suele estar instalado desde la construcción del edificio y puede ser probado en búsqueda de seccionamientos o cortes con equipos especializados para tales fines.

Cableado de redes: Este cableado es más sensible a perturbaciones electromagnéticas ya que transmite datos, por lo que debe estar prudentemente alejado del cableado eléctrico. Estas perturbaciones no las sufre el cableado de fibra óptica. Mantenerse al día en estándares de cableado estructurado ayuda a que la operación transcurra con menores sobresaltos dada su calidad actualizada. Se le aplican las mismas consideraciones sobre entubado y protección contra cortes y usuarios malintencionados.

3.5.3 Procedimientos de control para equipos remotos

La computación remota puede incluir cualquier equipo no localizado como equipos conectados remotamente a una red y equipos móviles. Para los propósitos de la seguridad física las preocupaciones sobre este tipo de dispositivos no se centra en su entorno sino, por su capacidad de

estar continuamente conectados y autenticados, en que mientras estén en ese estado no sean desatendidos permitiendo potencialmente a usuarios no autorizados ganar acceso a datos y sistemas de la organización. Los dispositivos móviles son muy vulnerables a robos o pérdidas lo que representa una gran vulnerabilidad de acceso no autorizado a los sistemas de la organización. Las consideraciones sobre los procesos de aseguramiento de dispositivos de conexión remota son las siguientes: [7]

- ✓ ¿Cómo son desconectados los usuarios cuando están inactivos en los sistemas?
- ✓ ¿Cómo se administran las cuentas de usuario y contraseñas en dispositivos remotos?
- ✓ Se tiene en cuenta la protección estructural y medio ambiental de los dispositivos remotos.
- ✓ Se tienen en cuenta controles de acceso para dispositivos remotos.
- ✓ Se incluyen etiquetas de propiedad y otros sistemas de identificación para dispositivos remotos.
- ✓ ¿Qué tratamiento se le da a los equipos descontinuados y quien es responsable de su descontinuación?

Políticas de seguridad: Frente a los equipos móviles y equipos portátiles es importante idear, implementar y explicar a los usuarios políticas de responsabilidad y uso de estos equipos. Aparte del valor económico de los equipos, muchas veces estos cargan información importante e incluso crítica de la organización, y al estar en constante traslado, sobre todo fuera de la organización, debe existir mucha conciencia entre los usuarios y una fuerte apropiación de las políticas y buenas prácticas de auto cuidado, seguridad y responsabilidad. Lo recomendable es que estos equipos no porten información muy importante, sino que en su lugar el usuario acceda a esta información conectándose remotamente a la red de la empresa y cargarla desde allí, esto para evitar que la información importante quede almacenada en equipos susceptibles a robos y pérdidas. En caso de un incidente es importante que el usuario reporte inmediatamente a la empresa para poder aplicar correctivos de emergencia; pero de cualquier modo tanto para cuidar los equipos y la información de caer en manos de personas no autorizadas o de ser manipulada malintencionadamente por el usuario mismo, las políticas de responsabilidad y compromiso con ellas son una protección prioritaria. Los equipos móviles suelen tener menos información crítica pero si más datos personales que pueden ser usados para realizar ingeniería social; las políticas deben educar en el no almacenamiento de datos de contacto, personales y contraseñas en dispositivos móviles.

3.5.4 Procedimientos de control para equipos de escritorio

Los equipos de escritorio siempre suponen múltiples tipos de problemas de seguridad: Hay que preocuparse por asegurar que personal no autorizado acceda, remueva, traslade, abra o manipule los equipos de escritorio y su información. Su colocación también debe ser pensada para prevenir que personas no autorizadas puedan leer el contenido desplegado en pantallas. Las consideraciones sobre los procesos de aseguramiento de equipos de escritorio son las siguientes: [7]

- ✓ Colocación segura y protección de equipos en las oficinas u otras áreas de trabajo.
- ✓ Proveer protección para cableado, conectores y otros cables que conecten dispositivos a la red.
- ✓ ¿Cómo son desconectados los usuarios cuando están inactivos en los sistemas?
- ✓ Lista de medidas de protección ambientales y estructurales para equipos de escritorio.
- ✓ Se incluyen etiquetas de propiedad y otros sistemas de identificación para equipos de escritorio.
- ✓ Se tiene en cuenta la seguridad de las cajas de los equipos para impedir la entrada no autorizada a los sistemas, así como la eliminación o la instalación de elementos como memorias, boards, puertos, etc.
- ✓ Lista de procedimientos contra robo.
- ✓ ¿Cómo están protegidos los equipos de escritorio ante subidas de tensión o cortes de energía?
- ✓ ¿Qué tratamiento se le da a los equipos descontinuados y quien es responsable de su descontinuación?

Políticas de seguridad: Los dispositivos de escritorio como PC, impresoras, faxes, teléfonos, entre otros, no son fáciles de asegurar ya que su buen o mal uso depende exclusivamente del usuario responsable de cada uno. Sólo la adopción de políticas claras y concretas de responsabilidad y uso pueden ayudar a reducir riesgos; y dado que estas políticas aplicarán a la mayoría del personal de la organización es importante que su claridad y enseñanza sean óptimas, para que se logre una buena aprehensión de los temas de seguridad sin quitar demasiado tiempo laboral a los empleados.

Privilegios: Le corresponde también al personal encargado de seguridad e IT definir muy bien, de acuerdo al rol y el área de cada usuario, los privilegios que tendrán estos y sus equipos en los sistemas de la organización. Definir cuentas de usuario con contraseñas personalizadas, acceso a

determinadas páginas o segmentos de la red interna, bloquear o desbloquear puertos para lectoescritura, etc. son privilegios que varían según las necesidades y condiciones de cada usuario y deben estar bien definidas y documentadas.

Cajas y dispositivos externos: Las cajas de los equipos de escritorio suelen carecer de todo tipo de medidas de seguridad e incluso conforme avanza la tecnología son más fáciles de abrir. Cambiar las cajas de todos los equipos por otras más seguras es costoso, por lo que es recomendable sellarlas lo que si bien no impide que sean abiertas, al menos demuestra que fueron alteradas. Otra alternativa es taladrar las cajas y montar un soporte para un candado; lo importante es manejar muy bien el cuidado de las llaves en caso de requerirse mantenimiento.
Aunque son poco usuales, es importante tener en consideración la existencia de aparatos como los keycatchers y otros sistemas de captación de datos, que aunque son engorrosos y fáciles de detectar, pueden no ser fácilmente reconocidos por algunos usuarios y pasar desadvertidos robando información.

Puertos y Dongles USB: En muchos casos la seguridad implica que los usuarios no puedan extraer información por medios digitales de su equipo de escritorio. Un bloqueo de puertos USB puede bastar para ello. Además de los puertos universales hay otros puertos como el Serial, que si bien no son comunes para la extracción de información, pueden ser adaptados para ello con un poco más de conocimiento. Una buena administración de estos puertos o incluso un bloqueo físico puede ayudar a mitigar riesgos ya que existen aparatos muy pequeños que pueden ser camuflados tras conectarse y extraer información. Este es el caso de los dongles USB que pueden transmitir información entre equipos con tan solo una conexión USB.

3.5.5 Procedimientos de control para telecomunicaciones y equipos de comunicaciones de datos.

Entre los equipos de telecomunicaciones y comunicaciones de datos se encuentran los switches, routers, hubs, teléfonos, PBXs, sistemas de correo de voz, e impresoras compartidas independientemente de su ubicación. Los equipos más costosos suelen estar en los centros de cómputo o en sus alrededores; de cualquier modo, dependiendo de cómo y donde estén instaladas las redes, bien puede haber una amplia variedad de equipos distribuidos por las oficinas, almacenes o áreas de manufactura. Las consideraciones sobre los procesos de aseguramiento de telecomunicaciones y equipos de comunicaciones de datos son las siguientes: [7]

- ✓ Proveer una colocación segura y protección de equipos en oficinas, otras áreas de trabajo, áreas de cableado y conexiones, y en el centro de cómputo.
- ✓ Usar etiquetas y sistemas de identificación adecuadas para los equipos de telecomunicaciones y comunicación de datos.
- ✓ Lista de tipos de puertas y cerraduras usados para asegurar áreas de telecomunicaciones y equipos de comunicación de datos, al igual que los tipos de racks o equipos de montaje que deben ser usados para instalar los equipos.
- ✓ ¿Qué tipos de alarmas y sistemas de monitoreo son utilizados para controlar el acceso a los equipos de telecomunicaciones y comunicación de datos?
- ✓ ¿Quién puede autorizar accesos a las áreas de los equipos de telecomunicaciones y comunicación de datos?
- ✓ ¿Cómo son monitoreados los proveedores de servicios cuándo y si necesitan acceder a las áreas de telecomunicaciones y equipos de comunicación de datos?
- ✓ ¿Cómo es el acceso a los equipos de telecomunicaciones y comunicación de datos para su mantenimiento?
- ✓ ¿Cómo son administradas y controladas las llaves y códigos de acceso a los equipos de telecomunicaciones y comunicación de datos?
- ✓ ¿Cómo y cuándo son revisados los logs de registro de voz y cómo se manejan los reportes de mal uso?
- ✓ ¿Qué tratamiento se le da a los equipos descontinuados y quien es responsable de su descontinuación?

3.5.6 Procedimientos de control para sistemas de vigilancia y alarma.

Muchas de las organizaciones más pequeñas no tienen mucho implementado en la vía de la vigilancia y los sistemas de alarma. Sin embargo la mayoría de las organizaciones más grandes tienen en funcionamiento algún tipo de sistema de vigilancia y alarmas. Estos sistemas son prácticamente inútiles si pueden ser accesados y desactivados, por lo que, actualmente, la mayoría de estos sistemas son computarizados y controlados por software que corre en equipos de escritorio y pequeños servidores. Por lo tanto, es aconsejable desarrollar procedimientos apropiados para asegurar tanto la vigilancia y el control, como el funcionamiento y la estructura propios de estos sistemas, y estos procedimientos deben estar en concordancia con los procedimientos de seguridad de equipos de IT. Los procedimientos de aseguramiento de sistemas de vigilancia y alarmas son

muy parecidos a los de los equipos de telecomunicaciones y equipos de comunicación de datos y sus consideraciones son las siguientes: [7]

- ✓ Proveer una colocación segura y protección de sistemas de vigilancia y alarmas en oficinas, otras áreas de trabajo, vestíbulos, y en áreas exteriores.
- ✓ Proveer protección para cableados, conectores y otras conexiones de los sistemas de vigilancia y alarmas con las redes internas o externas usadas para notificar las emergencias y solicitar los servicios correspondientes.
- ✓ Usar etiquetas y sistemas de identificación adecuadas para los sistemas de vigilancia y alarmas.
- ✓ Lista de tipos de puertas y cerraduras usados para asegurar áreas de sistemas de vigilancia y alarmas.
- ✓ ¿Quién puede autorizar accesos a las áreas los sistemas de vigilancia y alarma y cómo son administrados sus logs de registro?
- ✓ ¿Cómo son monitoreados los proveedores de servicios cuándo y si necesitan acceder a las áreas de los sistemas de vigilancia y alarma?
- ✓ ¿Cómo son administradas y controladas las llaves y códigos de acceso a los equipos de vigilancia y alarma?
- ✓ ¿Qué tratamiento se le da a los equipos descontinuados y quien es responsable de su descontinuación?

Estas recomendaciones de control dan paso a la etapa final del proceso de evaluación de riesgos: La mitigación de riesgos donde los procesos de control técnicos y de procedimiento son evaluados, priorizados e implementados y sobre esa base se hace un nuevo análisis de riesgos para determinar el riesgo residual. Es importante subrayar que no todos los controles son aplicables o viables. Un análisis de costo-beneficio es fundamental en la elección de controles en la medida en que su desarrollo e implementación sean acordes al esfuerzo económico y de trabajo que exigen los activos y sistemas para su protección; no es justificable implementar un control que valga más que el activo a proteger.

3.6 Mitigación de riesgos y riesgo residual

Aquí se prosigue con el proceso de gestión de riesgos. La mitigación de riesgos implica priorizar, evaluar e implementar los controles de reducción de riesgo inherente para el proceso de gestión de riesgos.

Dado que eliminar completamente un riesgo es impráctico o usualmente imposible hay que enfocarse en las soluciones menos costosas e implementar los controles más apropiados para reducir el nivel de riesgo de los activos a un nivel aceptable, que implica que la organización aprenda a vivir con ellos bajo la base de tener el mínimo impacto adverso al negocio y su misión.

3.6.1 Opciones de mitigación de riesgos

De acuerdo a las particularidades de cada riesgo, su impacto, sus controles, el costo de su impacto y el costo de sus controles se toman deben tomar decisiones para el tratamiento de cada uno. Estas decisiones pueden ser: [2]

- ✓ **Tolerar el Riesgo:** La exposición del activo al riesgo es tolerable sin que se tome ninguna acción al respecto. Esta es una opción de mitigación cuando el costo del tratamiento del riesgo es mayor al beneficio obtenido por el aseguramiento del activo o del activo mismo. Esta opción, por supuesto, debe ser complementada con un plan de contingencia para manejar el impacto en caso de que el riesgo se manifieste.
- ✓ **Tratar el Riesgo:** Esta debe ser la opción que se elija para la mayoría de riesgos. El propósito del tratamiento de los riesgos es que mientras las actividades de la organización continúan desarrollándose, se toman medidas para llevar los riesgos a niveles tolerables. Estas medidas son los controles definidos en la sección anterior.
- ✓ **Transferir el Riesgo:** Para algunos riesgos la mejor opción puede ser transferirlos a un tercero. Puede haber transferencia adquiriendo un seguro convencional o pagando a un tercero para que comparta o tome el riesgo. Esta es una opción particularmente útil para riesgos financieros. La transferencia de riesgos es considerada bien para reducir la exposición de la organización o porque otra organización tiene mejores capacidades de manejar efectivamente los riesgos. Es importante anotar que no todos los riesgos pueden ser transferibles en un 100% como es el caso de los riesgos de reputación. Es importante definir muy bien los criterios con el tercero para que al compartir el riesgo este quede cubierto totalmente entre las organizaciones.
- ✓ **Terminar el riesgo:** Algunos riesgos solo son tratables o contenibles en un nivel aceptable dando término a la actividad. Esta opción debe ser únicamente escogida luego de haber

estudiado la efectividad de las otras opciones y sus costos, y haberlas descartado completamente. Es importante también anotar que aunque un análisis juicioso recomiende terminar alguna actividad, hay actividades que no son terminables y hay que tomar otra opción aunque no resulte óptima.

3.6.2 Definición de niveles de efectividad de controles

En caso de que se elija la opción de tratar el riesgo es imperioso evaluar la efectividad que supone la implementación del control o la efectividad que supondría implementarlo. Los valores de la siguiente tabla muestran la definición de la escala de la efectividad de los controles:

Escala Cualitativa	Escala Cuantitativa	Descripción
Deficiente	5	No existe o no se ha implementado el control
Malo	4	El control existe pero no es efecivo
Aceptable	3	El control existe y es efectivo pero no se aplica debidamente
Bueno	2	El control se aplica debidamente pero no es 100% eectivo
Excelente	1	El control se aplica debidamente y es 100% eectivo

Tabla 40: Tabla de valoración de eficiencia de controles

3.6.3 Riesgo residual

El grado de riesgo puede ser analizado sobre la reducción generada por los controles nuevos o los controles mejorados al impacto o a la probabilidad de materialización de una amenaza, los dos parámetros que determinan el nivel de riesgo de un activo de información.
Los nuevos controles o los controles mejorados pueden mitigar riesgos por medio de:

- Eliminar algunas de las vulnerabilidades de los activos y sistemas reduciendo el número de posibles parejas fuente de amenaza – vulnerabilidad.
- Adicionando controles orientados a reducir la capacidad y motivación de una fuente de amenaza.
- Reduciendo la magnitud del impacto adverso limitando el grado de vulnerabilidad o modificando la relación del activo con la misión de la organización.

El riesgo remanente tras la implementación de controles nuevos o la mejora de los existentes es el riesgo residual. Prácticamente ningún riesgo sobre un activo de información puede ser eliminado pero la administración de riesgos direcciona a reducir el riesgo a los niveles óptimos de aceptación.

3.6.4 Matriz de niveles de riesgo residual

A diferencia de la matriz de cálculo del riesgo inherente, la matriz de riesgo residual está en función del nivel de riesgo inherente y la efectividad de los controles. El riesgo inherente lo conocemos ya por lo calculado en la fase 2 de la presente guía. Ahora, utilizando los valores definidos para la eficiencia de los controles en la sección 3.6.2 se define la matriz de riesgo residual.

- **Nivel Riesgo Inherente:** Muy Alto = 5, Alto = 4, Medio = 3, Bajo = 2, Muy Bajo = 1
- **Efectividad de Controles:** Deficiente = 5, Malo = 4, Aceptable = 3, Bueno = 2, Excelente = 1

Así, la matriz de riesgo inherente queda definida de la siguiente manera:

Matriz de determinación de Riesgo Residual		Nivel de Riesgo Inherente				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Efectividad de Controles	Excelente	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo
	1	1 x 1 = 1	2 x 1 = 2	3 x 1 = 3	4 x 1 = 4	5 x 1 = 5
	Bueno	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	Bajo
	2	1 x 2 = 2	2 x 2 = 4	3 x 2 = 6	4 x 2 = 8	5 x 2 = 10
	Aceptable	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Medio
	3	1 x 3 = 3	2 x 3 = 6	3 x 3 = 9	4 x 3 = 12	5 x 3 = 15
	Malo	Muy Bajo	Muy Bajo	Bajo	Medio	Alto
	4	1 x 4 = 4	2 x 4 = 8	3 x 4 = 12	4 x 4 = 16	5 x 4 = 20
	Deficiente	Muy Bajo	Bajo	Medio	Alto	Muy Alto
	5	1 x 5 = 5	2 x 5 = 10	3 x 5 = 15	4 x 5 = 20	5 x 5= 25

Tabla 41: Matriz de riesgo residual

La escala de riesgos de la matriz es:

Riesgo	Valor Mínimo	Valor Máximo
Muy Bajo	1	9
Bajo	10	14
Medio	15	19
Alto	20	24
Muy Alto	25	

Tabla 42: Tabla de valoración de escalas de riesgo residual

El riesgo residual es el vestigio que queda después de haber tratado los riesgos con los diferentes controles que dieran lugar. Este riesgo que persiste ya no es mitigable y la opción que queda es tolerarlo. Si el impacto continúa siendo crítico queda a discreción de la organización definir si terminar la actividad para finalizar el riesgo u optar por la transferencia aun cuando el costo sea alto pero la actividad sea fundamental para el negocio.

3.7 Resumen de la Fase III

La Fase III consta de las siguientes acciones

Lista de chequeo acciones Fase III		
No.	**Actividad**	**¿Realizada?**
1	Conocidas las vulnerabilidades que permitieran explotar una amenaza y el riesgo inherente de que esto suceda a los activos de información se procede a plantear los controles de mitigación. Para esto El proceso de documentación basado en los registros de las plantillas de las Fases I y II debe estar de preferencia finalizado.	
2	Realizar una evaluación del perímetro y las instalaciones:	
2.1	**Vecindario**: Situación local socio politico económica y vias de acceso. Rasgos topográficos y servicios públicos disponibles. Otras empresas en el sector.	
2.2	**Barrera Perimetral:** Cercas, muros, alambrados, alumbrado y marcas de escalamiento. Su estado, su situación de aseo y los materiales utilizados . Peligros que representan.	
2.3	**Áreas Intermedias abiertas:** Estacionamientos, obstáculos, personal errante. Alarmas externas y funcionamiento. Personal de vigilancia, rondas y tiempos. Equipos de utilería y armamentos del personal de vigilancia. Situación económica del personal de vigilancia. Entrada de vehículos de personal y entrada y salida de mercancías y basuras.	
2.4	**Muros periféricos de las instalaciones:** Estado de puertas y ventanas. Accesos principales, secundarios y ocultos o subterráneos. Control de llaves, candados y alarmas.	
2.5	**Áreas internas:** Accesos de personal, información de orientación, control de paquetes y vehículos. Carnetización. Registro de bolsos y paquetes e información a visitantes. Zonas públicas y privadas y sus accesos. Rutas de evacuación	

Lista de chequeo acciones Fase III		
No.	**Actividad**	**¿Realizada?**
1	Conocidas las vulnerabilidades que permitieran explotar una amenaza y el riesgo inherente de que esto suceda a los activos de información se procede a plantear los controles de mitigación. Para esto El proceso de documentación basado en los registros de las plantillas de las Fases I y II debe estar de preferencia finalizado.	
2	Realizar una evaluación del perímetro y las instalaciones:	
2.1	**Vecindario**: Situación local socio politico económica y vias de acceso. Rasgos topográficos y servicios públicos disponibles. Otras empresas en el sector.	
2.2	**Barrera Perimetral:** Cercas, muros, alambrados, alumbrado y marcas de escalamiento. Su estado, su situación de aseo y los materiales utilizados . Peligros que representan.	
2.3	**Áreas Intermedias abiertas:** Estacionamientos, obstáculos, personal errante. Alarmas externas y funcionamiento. Personal de vigilancia, rondas y tiempos. Equipos de utilería y armamentos del personal de vigilancia. Situación económica del personal de vigilancia. Entrada de vehículos de personal y entrada y salida de mercancías y basuras.	
2.4	**Muros periféricos de las instalaciones:** Estado de puertas y ventanas. Accesos principales, secundarios y ocultos o subterráneos. Control de llaves, candados y alarmas.	
2.5	**Áreas internas:** Accesos de personal, información de orientación, control de paquetes y vehículos. Carnetización. Registro de bolsos y paquetes e información a visitantes. Zonas públicas y privadas y sus accesos. Rutas de evacuación	
3	Realizar una evaluación sobre las instalaciones o edificios y sus características físicas.	
3.1	**El suministro eléctrico:** Servicio de la empresa de energía y regularidad y calidad del servicio. Plantas y equipos auxiliares en caso de falla eléctrica. Tiempos de abastecimiento de emergencia. Planes de contingencia y continuidad. Acceso a las fuentes de suministro	
3.2	Acceso físico a las instalaciones: Definición de horarios y personal autorizado. Tipos de cerraduras y alarmas o sensores según las zonas. Protección de la información de acuerdo a prioridad y zonas. Revisión de ductos de ventilación.	

3.3	**Controles contra Incendios e Incidentes:** Extintores debidamente colocados y personal entrenado en su uso. Buen estado de extintores y recargas vigentes. Pruebas periódicas de alarmas contra incendios y simulacros. Simulacros y buena orientación espacial y de procedimientos en caso de terremoto.	
3.4	**Control de warchalking:** Control de merodeadores y marcas en muros. Protección de redes internas y salidas a internet. Arquitectura de redes con Zona DMZ y privada. Controles de acceso a redes. Perfiles y contraseñas	
4	Realizar una evaluación de seguridad física sobre el entorno de los activos de información y los activos mismos.	
4.1	Control sobre centros de cómputo: Seguridad periférica del edificio o sección. Controles de acceso (roles, privilegios, mecanismos de autenticación, sensores de movimiento, registros de acceso). Aseguramiento de equipos y cableados sobre estándares y buenas prácticas. Backups de información y soportes de respaldo para funcionamiento y control de incidentes (ventilación, control de incendios, etc.) , Registro de logs y seguimiento y monitoreo continuo.	
4.2	Control sobre conexiones y cableados: Condiciones electromagnéticas del entorno, estándares de instalación y monitoreo de caleado y conexiones. Accesos a personal de mantenimiento y personal externo prestador de servicios. Tipos de cajas y cuartos, sus accesos y cerraduras. Alejamiento de humedades y contacto con agua. Registro de accesos a manipulación de cableados y conexciones.	
4.3	Control sobre equipos remotos: Condiciones de conexión a la red interna bajo inactividad de usuarios fuera del edificio. Controles de acceso y autenticación. Políticas en caso de extravío o robo.	
4.4	Control sobre equipos de escritorio: Protección de cableados, conexiones, cajas y puertos. Control de acceso a usuarios, manejo de contraseñas y tiempos de inactividad. Control sobre cambios ambientales y eléctricos, control de incidentes y redundancia de información.	
4.5	Control sobre telecomunicaciones y equipos de telecomunicaciones: Condiciones de cableado y suministro eléctrico. Control sobre comunicaciones permitidas y no permitidas. Control de acceso y registros de acciones de usuarios. Controles de acceso especial en caso de áreas específicas de funcionamiento de equipos de telecomunicaciones.	
4.6	Control sobre sistemas de vigilancia y alarma: Sistemas de vigilancia y alarma funcionando correctamente. Programas de simulacros. Capacitación de personal en su uso y procedimientos. Control de accesos a configuración de personal interno y de mantenimiento externo de prestadores de servicios. Registros de acciones. Control de falsas alarmas.	
5	Sobre los controles propuestos definir opciones para tratar los riesgos.	
6	Determinación del riesgo residual tras la evaluación de funcionalidad de los controles aplicados.	

Tabla 43: Lista de chequeo acciones Fase III

4. Fase IV: Revisión y Documentación

Esta fase de la metodología es en realidad transversal a las tres fases definidas atrás. Con el fin de que la administración de riesgos y el buen aseguramiento físico de la organización sea un proceso ordenado y sistemático, debe procurarse que en cada etapa de los procedimientos anteriormente definidos se vaya generando un reporte escrito de la información levantada.

En primera instancia al entrar a la organización y desarrollar las entrevistas que se consideren pertinentes, llevar un registro claro de las explicaciones de los encargados de control. Solicitar la información pertinente respecto al funcionamiento de la empresa, su organización y sectorización, su normatividad y políticas, la legislación vigente que le rige y sus expectativas respecto al aseguramiento físico. Esto ayudará a conocer bien el ambiente de trabajo y las pautas fundamentales para la aplicación de la guía.

Esta guía cuenta con las plantillas necesarias para desarrollar todo el proceso de administración de riesgos de una manera ordenada. Utilizarlas adecuadamente ayudará a llevar un proceso de aseguramiento ordenado y estructurado, donde, en la medida de que el volumen de información vaya aumentando, se pueda saber claramente qué es lo que se ha recolectado, cómo se ha sistematizado y hacia donde debe dirigirse el siguiente paso.

Una vez que el proceso de aseguramiento se ha completado, los resultados deben ser documentados en un reporte oficial. Estos reportes son el suministro para que la administración tome decisiones sobre la política, los procedimientos, el presupuesto, y los cambios y acciones que se tomen sobre los sistemas y activos. Distinto a un reporte de auditoría que informa sobre las malas acciones, un reporte de aseguramiento no debe presentarse de manera acusatoria sino como una aproximación analítica y sistemática al aseguramiento de riesgos con el fin de prever, limitar o reducir potenciales pérdidas o daños.

4.1 Resumen de la Fase IV

La Fase IV consta de las siguientes acciones

Lista de chequeo acciones Fase IV		
No.	**Actividad**	**¿Realizada?**
1	Documentación y revisión de procesos como proceso transversal a las tres fases anteriores.	
2	Registro de procesos en las plantillas seleccionadas para tal fin.	
3	Presentación de informes finales tras el proceso de aseguramiento y como soporte para los procesos periódicos futuros.	

Tabla 44: Lista de chequeo acciones Fase IV

ESTÁNDARES Y NORMAS RECOMENDADAS

Aquí Se encuentran algunas normas recomendadas para el diseño e implementación de planta física segura de acuerdo a estándares internacionales:

Estándares para Data Centers

- ANSI/BICSI 002. Diseño de data centers e implementación de buenas prácticas. Disponible en: https://www.bicsi.org/uploadedfiles/bicsi_002_sample.pdf (Versión gratuita) [15]
- ANSI/TIA 942. Infraestructura de telecomunicaciones para data centers. Disponible en: http://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=TIA-942 (Versión paga) [10]
- NFPA 75. Estándar para la protección de tecnología de equipos de información. 2013. Disponible en: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=75 (Versión paga) [16]
- Norma Técnica Colombiana 2050. Disponible en: http://ingenieria.bligoo.com.co/media/users/19/962117/files/219177/NTC_2050.pdf (Versión Gratuita) [17]

- TIA 568. Estándar de cableado para instalaciones comerciales. Disponible en: http://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=TIA-568 (Versión paga) [18]

Estándares para Sistemas de Telecomunicaciones

- Estándar R56 de Motorola. Disponible en: http://www.radioandtrunking.com/downloads/motorola/R56_2005_manual.pdf (Versión Gratuita) [19]
- NFPA 76. Estándar para la protección contra fuego de equipos de telecomunicaciones. 2013. Disponible en: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=76 (Versión paga) [14]

Otros estándares recomendados

- NFPA 101. Código de seguridad humana. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/930/8/nfpa_101_-_codigo_de_seguridad_humana_-_2000_edition.pdf (Versión Gratuita en español) [20]
- NFPA 70. Código nacional eléctrico. Disponible en: https://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=70 (Versión paga) [21]
- NFPA 72. Código nacional de alarmas de incendio. Disponible en: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=72 (Versión paga) [22]
- NFPA 10. Estándar para los extintores de fuego portátiles. Disponible en: https://law.resource.org/pub/us/cfr/ibr/004/nfpa.10.2002.pdf (Versión gratuita) [23]
- NFPA 12. Estándar de sistemas de extinción de dióxido de carbono. Disponible en: https://law.resource.org/pub/us/cfr/ibr/004/nfpa.12.2005.pdf (Versión gratuita) [24]
- NFPA 780. Estándar para a protección contra rayos y descargas eléctricas. Disponible en: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=780 (Versión Paga) [25]

REFERENCIAS BIBLIOGRÁFICAS

[1] P. F. Drucker, "Detrás de la revolución de la información," *Rev. Factoría Oct.-Enero*, no. 13, 2001.
[2] H. M. Treasury, "The Orange Book: management of risk–principles and concepts," *Lond. HM Treas.*, 2004.
[3] S. NIST, "800-30," *Risk Manag. Guide Inf. Technol. Syst.*, pp. 800–30, 2002.
[4] C. S. de Administración Electrónica, *MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.-España. Fecha de consulta: 1 de abril de 2010.* .
[5] MinCIT. Ministerio de comercio, Industria y Turismo, "Definición Tamaño Empresarial Micro, Pequeña, Mediana o Grande." .
[6] O. I. de Normalización, *ISO/IEC 27002: Information Technology, Security Techniques, Code of Practice for Information Security Management*. ISO/IEC, 2005.
[7] M. Erbschloe, *Physical security for IT*. Access Online via Elsevier, 2004.
[8] Vallejo Rosero, Silvio, *Seguridad privada; Manual operacional para el planeamiento, desarrollo y control de programas de seguridad*, Primera. Pasto. Nariño. Colombia: Graficolor, 1996.
[9] López Hernández, José María, "Seguridad Fisica COMO." 2004.
[10] Chris DiMinico & Jonathan Jew, "ANSI/TIA-- 942 Telecommunications Infrastructure Standard for Data Centers." 2005.
[11] Chris DiMinico (IEEE 802.3 HSSG), "Telecommunications Infraestructure Satandard for Data Centers."
[12] Carlos Iván Zuluaga Vélez, RCDD. GZ Ingeniería, "NORMATIVIDAD Y TECNOLOGIA DE PROTECCIÓN DE INCENDIOS EN CENTROS DE COMPUTO Y TELECOMUNICACIONES."
[13] Telecommunications Inc, "Como diseñar un centro de Datos óptimo." 2005.
[14] Nationa Fire Protection Association, "NFPA 76. Estándar para la protección contra el fuego de instalaciones de telecomunicaciones." 2012.
[15] Jonathan Jew & John Kacperski, "ANSI/NECA/BICSI-002 Data Center Design and Implementation Best Practices." 2007.
[16] Nationa Fire Protection Association, "NFPA 75: STANDARD FOR THE FIRE PROTECTION OF INFORMATION TECHNOLOGY EQUIPMENT." 2013.
[17] ICONTEC, "Norma Técnica Colombiana 2050." 1998.
[18] Chris DiMinico & Jonathan Jew, "TIA-568. Commercial Building Cabling Standard." 2012.
[19] Motorola, Inc., "MOTOROLA R56.STANDARDS AND GUIDELINES FOR COMMUNICATION SITES." 2005.
[20] N. F. P. A. Instituto Argentino de Normalización, "NFPA 101. Código de Seguridad Humana." 2000.
[21] Nationa Fire Protection Association, "NFPA 70: National Electrical Code." 2014.
[22] Nationa Fire Protection Association, "NFPA 72. National Fire Alarm and Signaling Code." 2013.
[23] Nationa Fire Protection Association, "NFPA 10. Standard for Portable Fire Extinguishers." 2002.
[24] Nationa Fire Protection Association, "NFPA 12. Standard on Carbon Dioxide Extinguishing

Systems.” 2005.
[25] Nationa Fire Protection Association, “NFPA 780. Standard for the Lightning Protection Systems.” 2014.

PLANTILLAS PARA EL PROCESO DE ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

CIS1310SD02

FELIPE BAYONA BORRERO

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C
2013

PLANTILLAS PARA EL PROCESO DE ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN EN PYMES

CIS1310SD02

AUTOR
FELIPE BAYONA BORRERO

HTTP://PEGASUS.JAVERIANA.EDU.CO/~CIS1310SD02

DIRECTOR
ING. JOSHSUA JAMES GONZALEZ DIAZ

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C
2013

Contenido

Índice de tablas

1. Introducción

En este documento se encuentra recogidas las plantillas auxiliares al proceso de administración de riesgos de la guía metodológica.
Su intención es servir de herramienta de registro y valoración, o como base para los formatos que las organizaciones diseñen para el registro de la información levantada y analizada dentro de todo el proceso de administración de riesgos de la seguridad física para los activos de información.

2. Plantillas para el levantamiento de activos de información

Las siguientes plantillas servirán a la organización para llevar registro de sus activos de información de acuerdo a la clasificación planteada en la Guía metodológica.
Todas las plantillas comparten la siguiente información:

- ✓ **Código**: Este debe ser único para cada activo de información. En caso de hacerse un levantamiento de activos por procesos es recomendable que el código lleve: una sigla que identifique el proceso + una sigla que identifique el tipo de activo + un número único consecutivo.
- ✓ **Nombre:** Es el nombre del activo.
- ✓ **Descripción:** Es una descripción breve del activo de información. Puede especificarse su uso y el proceso al que pertenece.
- ✓ **Propietario:** Es el nombre del usuario o área de la organización dueña del activo.
- ✓ **Custodio:** Es el usuario o área responsable de custodiar el activo.
- ✓ **Ubicación:** Es la ubicación física que tiene el activo dentro de la organización (en caso de tenerla).
- ✓ **Campos particulares:** Cada plantilla tiene en adelante campos particulares para clasificarlos según las directrices de la Guía metodológica. Aquí se debe marcar con una X la/s casilla/s correspondientes a la/s cualidad/des especifica/s de cada activo.

Las siguientes son las plantillas para el levantamiento de activos de información:

2.1 Plantilla de activos esenciales

Activos esenciales						
Codigo:		**Nombre:**				
Descripción:						
Propietario:						
Custodio:						
Ubicación:						
Clasificación	Vital		Personal		Confidencial	
					Nivel:	

Tabla 45: Plantilla de activos esenciales.

2.2 Plantilla de activos de información de funcionamiento

Información de funcionamiento						
Codigo:		**Nombre:**				
Descripción:						
Propietario:						
Custodio:						
Ubicación:						
Tipo:	Fichero		Backup		Datos de configuración	
	Datos de control de acceso		Registro de actividad (Log)		Código fuente, ejecutable o pruebas	

Tabla 46: Plantilla de activos de información de funcionamiento

2.3 Plantilla de servicios

Servicios						
Codigo:		**Nombre:**				
Descripción:						
Tipo:	Usuarios internos		Usuarios externos		Público	

Tabla 47: Plantilla de servicios

2.4 Plantilla de hardware

Hardware						
Codigo:		**Nombre:**				
Descripción:						
Propietario:						
Custodio:						
Ubicación:					**Cantidad:**	
Tipo:	Grande		Medio		PC	
	Movil		Virtual		Backup	
	Periférico		Red			

Tabla 48: Plantilla de hardware

2.5 Plantilla de redes de comunicación

Redes de comunicación						
Codigo:		**Nombre:**				
Descripción:						
Propietario:						
Custodio:						
Ubicación:						
Tipo:	Telefónica		Datos		Vigilancia	
	Punto a Punto		Radio		Inalámbrica	
	Movil		Satelital		Circuito cerrado	
	LAN		MAN		WAN	

Tabla 49: Plantilla de redes de comunicación

2.6 Plantilla de soporte de información

Soportes de información						
Codigo:		**Nombre:**				
Descripción:						
Propietario:						
Custodio:						
Ubicación:					**Cantidad:**	
Tipo:	Electrónico		Disco duro		Memoria USB	
			Disco virtual		Memoria Flash	
			CD ROM / DVD		Cinta/Diskette	
	No Electrónico		Impresión		Otro	

Tabla 50: Plantilla de soportes de información

2.7 Plantilla de equipos auxiliares

Equipos auxiliares						
Codigo:		**Nombre:**				
Descripción:						
Propietario:						
Custodio:						
Ubicación:					**Cantidad:**	
Tipo:	Fuente de alimentación		Generador Eléctrico		Equipo de aclimarización	
	UPS		Cable eléctrico		Fibra óptica	
	Suministros		Equipos		Moviliario	

Tabla 51: Plantilla de equipos auxiliares

2.8 Plantilla de instalaciones

Instalaciones						
Codigo:		**Nombre:**				
Descripción:						
Propietario:						
Custodio:						
Ubicación:					**Cantidad:**	
Tipo:	Edificio		Oficina		Local	
	Contenedor		Vehículo		Instalación respaldo	

Tabla 52: Plantilla de instalaciones

2.9 Plantilla de personal

Personal						
Codigo:		**Cargo**				
Nombres:						
Área					**Cantidad:**	
Tipo:	Interno		Externo		Administración	

Tabla 53: Plantilla de personal

3. Plantilla de valoración de activos de información

Esta plantilla es para la valoración de los activos de información levantados. Dicha valoración procede según lo especificado en la Guía metodológica.
Contienen la siguiente información:

- ✓ **Código:** Este debe ser un código consecutivo único. Se aconseja colocar un prefijo que indique valoración + el código del activo a valorar.
- ✓ **Nombre:** Este es el nombre del activo de información.
- ✓ **Criterio:** Esta es una matriz cuyas filas son cada uno de los 7 principios de la seguridad definidos en la guía metodológica y sus columnas la valoración de cada uno igualmente definida. Se deben rellenar con una X según el valor que tiene el activo en sus medidas de aseguramiento.
- ✓ **Tipo:** Público, privado o confidencial.
- ✓ **Costo:** Este es el valor monetario del activo (en caso de tenerlo).
- ✓ **Observaciones:** Estas son las observaciones que tengan lugar de acuerdo a la valoración del activo.

La siguiente es la plantilla para la valoración de activos de información:

Valoración de activos								
Codigo		**Nombre**						
Evaluación		Muy Bajo	Bajo	Medio	Alto	Muy Alto	No aplica	**Tipo**
Criterios	Integridad							Público
	Disponibilidad							
	Confidencialidad							Privado
	Autenticación							
	Autorización							Confidencial
	No repudiación							
	Observancia							Costo
Observaciones								$

Tabla 54: Plantilla de valoración de activos de información

4. Plantilla para listar amenazas

En el proceso de administración de riesgos pueden hallarse muchas amenazas. Tenerlas identificadas y ordenadas ayudará a documentar el proceso y valorar avances.

Para listar las amenazas encontradas se recomienda la siguiente información:

- ✓ **Código:** Es un identificativo único.
- ✓ **Tipo:** Según lo definido en la guía metodológica
- ✓ **Descripción:** Aquí se describe la amenaza y su fuente identificada.

La siguiente es la plantilla para listar amenazas:

Lista de amenazas identificadas					
Código	Natural	Entorno	Humana		Fuente de amenaza / Descripción
			Involuntaria	Voluntaria	

Tabla 55: Plantilla para listar amenazas

5. Plantilla para cálculo de riesgo inherente

Esta plantilla ayuda a documentar el cálculo del riesgo inherente en función del impacto de la materialización de una vulnerabilidad causada por una amenaza y su probabilidad de ocurrencia.
Esta plantilla recoge la siguiente información:

- ✓ **Código:** Identificador único del activo de información
- ✓ **Nombre:** Nombre del activo de información
- ✓ **Código de amenaza:** Identificador único de la amenaza disponible en la lista de amenazas obtenidas.
- ✓ **Vulnerabilidad:** Descripción de la vulnerabilidad que facilitaría la materialización de la amenaza.
- ✓ **Impacto:** Valores de impacto de la materialización de la amenaza según lo descrito en la guía.
- ✓ **Probabilidad:** Porcentaje de posibilidad de ocurrencia de la explotación de la vulnerabilidad.
- ✓ **Riesgo Inherente:** Valor del riesgo inherente de acuerdo a lo establecido en la guía.

La siguiente es la plantilla para el cálculo del riesgo inherente:

Determinación de Riesgo Inherente														
Codigo:		Nombre:												
Codigo Amenaza	Vulnerabilidad	Impacto									Probabilidad	Impacto total	Riesgo Inherente
		Integridad	Confidencialidad	Disponibilidad	Autenticación	Autorización	No repudiación	Observancia	Imagen	Dinero			

Tabla 56: Plantilla para el cálculo del riesgo inherente

6. Plantilla para listar controles

De acuerdo a la clasificación de controles presentado en la guía metodológica, el aconsejable armar un listado de controles sugeridos para contrarrestar las vulnerabilidades encontradas para cada activo.

Para listar controles recomendados se sugiere la siguiente información:

- ✓ **Código:** Este es un identificador único del control.
- ✓ **Tipo:** Según lo definido en la Guía metodológica.
- ✓ **Descripción:** Esto es el detalle del control a implementar.

La plantilla sugerida para listar controles es la siguiente:

Lista de controles sugeridos				
Código	Técnico	Administración	Operaivo	Descripción

Tabla 57: Plantilla para listar controles

7. Plantilla para cálculo de riesgo residual

Esta plantilla ayuda a documentar el cálculo del riesgo residual en función del riesgo inherente encontrado anteriormente y la efectividad del control sugerido para mitigarlo.
La plantilla recoge la siguiente información:

- ✓ **Código:** Este es el código del activo de información
- ✓ **Nombre:** Este es el nombre del activo de información.
- ✓ **Código Amenaza:** Identificador único de la amenaza disponible en la lista de amenazas obtenidas.
- ✓ **Vulnerabilidad:** Es la vulnerabilidad que sería explotada por la amenaza.
- ✓ **Código Control:** Es el identificador único del control sugerido para mitigar la vulnerabilidad
- ✓ **Control:** Es la descripción del control sugerido para mitigar la vulnerabilidad
- ✓ **Efectividad control:** Es la efectividad del control frente a la vulnerabilidad según lo especificado en la Guía metodológica
- ✓ **Riesgo Inherente:** Es el riesgo sin control de mitigación calculado anteriormente
- ✓ **Riesgo Residual:** Es el riesgo que permanece tras la aplicación del control. Se calcula según las pautas de la Guía metodológica

La siguiente es la plantilla para el cálculo del riesgo residual:

Determinación de Riesgo Residual							
Código:		Nombre:					
Código Amenaza	Vulnerabilidad		Código Control	Control	Efectividad Control	Riesgo Inherente	Riesgo Residual

Tabla 58: Plantilla para cálculo de riesgo residual