IMPORTANCIA DE CONTROLAR TODAS LAS AMENAZAS DETECTADAS A TRAVÉS DE MAGERIT V.3 E ISO/ IEC 27002 SEGÚN ANÁLISIS DE ATAQUES INFORMÁTICOS EN LATINOAMÉRICA

HUGO ALFONSO RODRÍGUEZ ARROYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2019

IMPORTANCIA DE CONTROLAR TODAS LAS AMENAZAS DETECTADAS A TRAVÉS DE MAGERIT V.3 E ISO/IEC 27002 SEGÚN ANÁLISIS DE ATAQUES INFORMÁTICOS EN LATINOAMÉRICA

HUGO ALFONSO RODRÍGUEZ ARROYO

Monografía

Asesor: Francisco Javier Hilarión Novoa
Docente Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2019

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Barranquilla, abril 20 de 2019

DEDICATORIA

Este documento está dedicado a Dios, por brindarme salud, la oportunidad de especializarme y por orientarme de manera especial con mis cuatro puntos cardinales, mi esposa Magaly Rojas y mis hijos Axel, Mathias y Mariangel.

AGRADECIMIENTO

Asesor: Francisco Javier Hilarión Novoa
Docente Especialista en Seguridad Informática.

Frey de Jesús Castro Ramírez
Ingeniero de Sistemas Especialista en Seguridad Informática
Magister en Administración y Planificación Educativa.

Bienestar Social de la Gobernación del Atlántico.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

SGSI: Un Sistema de Gestión de Seguridad de la Información se encarga de proteger la integridad, confidencialidad y disponibilidad de los activos informáticos a través de una serie de medidas y/o políticas orientadas a procesos, documentados, estandarizados y de estricto cumplimiento para la organización.

SEGURIDAD DE LA INFORMACIÓN: Todas las medidas y procedimientos (humanos y técnicos), adoptados para proteger la integridad, confidencialidad y disponibilidad de la información.

INTEGRIDAD: Permite asegurar que los datos no se han falseado[1].

CONFIDENCIALIDAD: No desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales)[2].

DISPONIBILIDAD: Que la información se encuentre accesible en todo momento a los distintos usuarios autorizados[3].

SEGURIDAD DE LOS DATOS: Los datos han adquirido un lugar importante como recurso corporativo, pues en cierta medida, gran parte del éxito de muchas organizaciones esta asociados al control y manejo que se les da a estos. Cuando se atenta contra la seguridad de los datos la capacidad de una compañía para seguir funcionado de manera normal se puede ver afectada[4].

---

[1] Costas, Santos, Jesús. *Seguridad informática*, RA-MA Editorial, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3228430.
[2] Ibíd., p. 22
[3] Ibíd., p. 22
[4] Guillenson, Mark. Administración de Bases de Datos. México. 2006. P. 271.

SEGURIDAD INFORMÁTICA: Proceso de prevenir y detectar el uso no autorizado de un sistema informático[5].

RIESGO INFORMÁTICO: La Real Academia Española define el riesgo como aquella contingencia o proximidad de un daño[6], entonces si asociamos la posibilidad de que algo ocurra y el perjuicio que podemos sufrir con la seguridad informática, estaríamos hablando de riesgo informático como toda vulnerabilidad o amenaza (física o lógica) que causa un daño a nuestro sistema (equipos o información) o lo que conocemos como activos informáticos.

VULNERABILIDAD: Vulnerabilidad es todo punto débil de un sistema, ya sea por su diseño, implementación u operación, a través del cual se puede materializar una amenaza.

AMENAZA: Todo evento (humano, natural o técnico) que pueda afectar los activos de información (datos o infraestructura).

ATAQUE INFORMÁTICO: Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información. [CESID:1997][7].

ISO: Son las siglas que definen la Organización Internacional para la Estandarización, este organismo regula las normas para la fabricación comercio y comunicación de todas las industrias y comercios en el mundo.

---

[5] Universidad de Valencia. ¿Qué es la seguridad informática y cómo puede ayudarme?. Valencia, 2016. Recuperado de https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/
[6] RAE. Definición de Riesgo. https://dle.rae.es/?id=WT8tAMI
[7] Centro Superior de Información de la Defensa, "Glosario de Términos de Criptología", Ministerio de Defensa, 3ª edición, 1997. Citado por Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 99

NTC: Organismo Nacional de Normalización de Colombia. Encargado de crear normas técnicas y la certificar normas de calidad.

MAGERIRT: Metodología de análisis y gestión de riesgos elaborada por el Ministerio de Hacienda y Administraciones Públicas de España.

HACKERS: Son normalmente informáticos, que quieren descubrir vulnerabilidades de los sistemas por gusto, sin motivación económica ni dañina[8].

CRACKERS: Iindividuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos, etcétera[9].

SNIFFERS: Se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet[10].

LAMMERS: Personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan[11].

NEWBIE: Son hackers que apenas se inician.

CIBERTERRORISTA: Son expertos informáticos que trabajan para países u organizaciones como espías si saboteadores informáticos[12].

---

[8] PONFERRADA, J. Citado por Ticarte.com, Tipos de ataques y atacantes en CiberSeguridad. [en línea] http://www.ticarte.com/contenido/tipos-de-ataques-y-atacantes-en-ciberseguridad, 2015.
[9] Gómez, Vieites, Álvaro. Seguridad en equipos informáticos, RA-MA Editorial, 2014. p 38
[10] Ibíd., p. 39
[11] Ibíd., .p 39
[12] PONFERRADA, J. Op. cit., p. 1

PROGRAMADOR DE VIRUS: Experto en programación redes y sistemas., que crean programas dañinos que afectan a aplicaciones y a sistemas[13].

CARDERS: Son personas que se dedican a ataques de sistemas de tarjetas como cajeros automáticos[14].

[13] PONFERRADA, J. Op. cit., p. 1
[14] PONFERRADA, J. Op. cit., p. 1

RESUMEN

Toda organización, pública o privada, establece su sistema de gestión de seguridad de la información – SGSI de acuerdo a sus necesidades, disponibilidad de recursos e incluso de la percepción del riesgo informático de sus altos ejecutivos. Cada compañía implementa a su acomodo los controles necesarios para minimizar, transferir o afrontar los riesgos informáticos que se puedan presentar.

Existen diferentes metodologías para la gestión del riesgo informático, pero este documento se realiza bajo la guía de Magerit Versión 3 elaborada por el Consejo Superior de Administración Electrónica de España; una guía que parte de la identificación de los activos de información, incluyendo datos, hardware, recurso humano y software a los que otorga un valor y luego identifica las amenazas, riesgos y vulnerabilidades de cada uno de estos activos. Aunque Magerit incluye también los controles que se aplican a cada riesgo hallado, se ha optado por explicar y referir los controles que proporciona la ISO-IEC 27002 del 2013 porque es una guía de buenas prácticas que describe objetivos de control así como los controles recomendables en cuanto a seguridad de la información.

La presente investigación tiene como objetivo principal revisar la importancia de los resultados de un análisis de riesgos informáticos para que los profesionales de la seguridad informática se concienticen que toda amenaza detectada debe ser controlada mediante el estudio de la metodología MAGERIT V.3 y la norma ISO/IEC 27002:2013 y su aplicación en Latinoamérica. Para evitar cualquiera de los ataques que pueda sufrir el sistema, es necesario disponer de recursos económicos, humanos y técnicos que permitan de cierto modo, proteger los activos informáticos.

INTRODUCCIÓN

El siglo XXI es sin duda para toda organización un reto en todo lo que tiene que ver con las tecnologías de información y las comunicaciones TIC'S, bien sea pública o privada, desde la más pequeña hasta las grandes multinacionales generan cierta dependencia por la cantidad de información que producen y que en muchos casos se convierte en el activo más representativo de la organización, siendo esta, la principal razón por la cual se invierten grandes sumas de dinero en equipos de cómputo, software, plataformas en la nube y todo tipo de dispositivos con capacidad de almacenar, procesar y resguardar la información.

Pero de la misma manera en que las compañías se sumergen dentro de la tecnología, se ha acrecentado la comunidad de atacantes (hackers, crackers, sniffers, lammers, newbie, carders, ciberterroristas, etc.) no solo ha crecido en número, sino que también, han evolucionado en las técnicas utilizadas; es así que en el informe presentado por Kaspersky[15] en agosto de 2018 durante la octava cumbre de analistas de seguridad informática para América Latina Kaspersky Lab, registró más de 746 mil ataques de malware diarios durante los últimos 12 meses en América Latina, lo que significa un promedio de 9 ataques de malware por segundo.

No es menester citar los reportes de otras entidades dedicadas a medir los ataques informáticos, puesto que todos coinciden en que el indicador es demasiado elevado, viéndose este sector obligado a contar en las organizaciones con personal preparado para contrarrestar todas las amenazas que a diario se presenten y poder blindar la compañía y proteger los activos informáticos, pero aunque este equipo sea altamente cualificado y pueda aplicar diferentes metodologías de análisis y gestión del riesgo informático, su trabajo tiene que

afrontar otro gran reto; la alta dirección, los gerentes, accionistas o en otras palabras quienes aprueban los recursos económicos, pues sin presupuesto no se podrá aplicar todos los controles requeridos para las amenazas detectadas.

Por lo anteriormente expuesto, el autor resalta el valor de los resultados obtenidos de un análisis de riesgos informáticos para que los profesionales de la seguridad informática se concienticen que toda amenaza detectada debe ser controlada, logrando como Jeimy J. Cano[16] propuso: “un modelo de gobierno de seguridad de la información, que busca incorporar a la investigación actual elementos novedosos y prácticos que apalanquen los esfuerzos actuales y motiven un cambio en la forma como conocemos y fundamentamos las reflexiones sobre la seguridad de la información en las organizaciones del siglo XXI”.

De este modo la importancia de la monografía es lograr que todas las personas que participan del gobierno de la seguridad, principalmente la alta dirección, tomen conciencia de las cifras de ataques informáticos en los últimos años y de la variación o transformación de las técnicas empleadas que golpean fuertemente a las organizaciones, al punto que algunas no logran sobreponerse ante un siniestro informático.

[15] Kaspersky Lab. (14 de Agosto de 2018). *https://latam.kaspersky.com*. (G. Saldaña, Editor) Recuperado el 25 de octubre de 2018, de https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

[16] Cano, J. J. Modelo PERIL, Repensando el gobierno de la seguridad de la información desde la inevitabilidad de la falla. En: *VII Congreso Iberoamericano de Sewguridad Informática*. Sangolqui (Quito): Universidad de las Fuerzar Armadas del Ecuador - ESPE. 2015. p. 13

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

La gestión del riesgo informático en empresas del sector público y privado de Latinoamérica se ha tornado en un reto difícil de administrar por dos factores claves: primero, el significativo aumento de los ataques informáticos y la evolución de las técnicas empleadas y, en segundo lugar, la poca credibilidad que le dan a este fenómeno los gerentes, accionistas y miembros de la alta dirección al momento de disponer los recursos necesarios para brindar protección a los activos de información.

Por esta situación los profesionales y especialistas en seguridad informática al momento de emplear metodologías de análisis de riesgo informático, como MAGERIT, llevan intrínsecamente impregnado en su chic (memoria) la idea de aplicar controles de la ISO 27002, solo a algunas de las amenazas detectadas (las de mayor impacto), dejando desprotegidos muchos o algunos de los hallazgos presentados en el análisis y esto es precisamente lo que viene generando consecuencias negativas a las organizaciones que han sido afectadas por aquellas intrusiones que consideraron poco lesivas, mientras que del otro lado los atacantes si encuentran una oportunidad para cometer un ataque; haciendo necesario volcar esta situación con directrices más exigentes al momento de aplicar controles y romper estos paradigmas mediocres de atención a las amenazas.

1.2 DESCRIPCIÓN DEL PROBLEMA

El análisis de riesgos informáticos es un insumo clave al momento de implementar medidas de protección sobre los activos de información de una organización; lo que se hace después con el informe del análisis es realmente un tema interesante

y de gran interés para el área de la seguridad informática, en el entendido que las compañías invierten fuertes sumas de dinero para proteger sus activos de información.

Muchas empresas que destinan parte de su presupuesto para la protección de la información y la seguridad de los sistemas informáticos utilizan el análisis de riesgos como una estrategia que les oriente al momento de desplegar controles de seguridad, no obstante, al momento de establecer medidas preventivas y correctivas como parte de una adecuada gestión de riesgos se enfocan en los activos esenciales y específicamente en los que al momento del análisis se presupone que afectan seriamente a la organización, y terminan dejando de lado aquellas pequeñas vulnerabilidades que generalmente se convierten en el punto central de un ataque que les ocasiona más que en un dolor de cabeza, perdida de información, perdida de reputación e indisponibilidad de servicios, entre otros.

1.3 FORMULACIÓN DEL PROBLEMA

Si una metodología de análisis de riesgos informáticos genera toda la información requerida para implementar salvaguardas y medidas protección:

¿Por qué aplicar controles a algunas vulnerabilidades y no a todas?
¿Qué pasa con los riesgos de “bajo perfil” que identificó el análisis?
¿La metodología de análisis me dice que atienda unos riesgos y otros no?

2. JUSTIFICACIÓN

De acuerdo a cifras reveladas por la compañía de seguridad informática Kaspersky[17], durante la séptima Cumbre Latinoamericana de Analistas de Seguridad, desarrollada en Buenos Aires (Argentina) en septiembre de 2017, durante el periodo enero-agosto de ese año, se registraron 677.000.000 de ataques cibernéticos en América Latina, reflejando un alza del 59% comparado con el 2016 y significa que cada hora se realizaron 117 ataques y, 33 cada segundo. El informe también indica que, Brasil, México y Colombia son los países que más ataques cibernéticos han sufrido en lo que va del 2017, incluyendo ataques realizados al estar conectados a internet y estando fuera de conexión.

En cantidad de ataques Brasil representa el 53% del total, mientras que México se ubicó en el segundo lugar con 17% y Colombia en el tercer lugar, con 9%. Zurich, una de las aseguradoras globales más importantes en el mundo, realizó un estudio global en colaboración con el centro de estudios Atlantic Council, en el cual revela que, la mayoría de los profesionales de seguridad informática no tienen del todo claro la manera en que una falla tecnológica podría evolucionar a convertirse en un riesgo a nivel organizacional[18].

Frente al problema descrito es necesario realizar un análisis que me permita expresar un punto de vista sobre las metodologías de análisis de riesgo MAGERIT V.3 y la norma ISO/IEC 27002:2013, los resultados que estas generan y por supuesto el rango de aplicación de las acciones que deben emprender las organizaciones tras los informes generados, las cuales deben apuntarle a lo crítico

[17] KasperskyLab. Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina. Argentina, 2017. https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

[18] ZURICH Insurance Group. Beyond Data Breaches: Global Interconnections of Cyber Risk: Risk Nexus. Atlantic Council, 2014. 32p.

(como normalmente ocurre), pero sin dejar de lado el resto de las variables, en el entendido que vulneración (grande o pequeña) es vulneración.

2.1 IMPORTANCIA DEL PROYECTO

La importancia de esta monografía se ve reflejada en la concientización que transmiten las cifras de ataques informáticos en los últimos años y que muestran un aumento relevante además de la variación o transformación de las técnicas empleadas y que golpean fuertemente a las organizaciones, tanto que algunas no logran sobreponerse ante un siniestro informático.

De igual modo, es altamente relevante entender que las diferentes metodologías de análisis y gestión del riesgo informático brindan un panorama amplio del nivel de vulneración de la organización y, de igual modo, existen los controles para cada uno de estos, así que todo gerente, administrador y/o accionista de una compañía logrará entender que si tiene 5 puertas y solo asegura 4, no estará ahorrando el 20% de la inversión en seguridad, sino que por el contrario estará a expensas de perder el 80% de lo invertido en la seguridad de las 4 puertas más los desastres causados por el atacante.

2.1.1 Ventajas

Este apartado de la monografía se realiza de forma muy sencilla y clara para que el lector pueda apropiarse de las ventajas que tiene una organización de cualquier tamaño al atender las recomendaciones y pautas plasmadas en este documento y que están relacionadas con un máximo aprovechamiento de los insumos o datos recolectados durante el análisis de riesgos informáticos y la mejor manera aplicar los controles a todo riesgo mediante el balanceo de costos.

La principal ventaja que ofrece este compilado monográfico es la certeza de que la gestión de incidentes efectiva hoy en día debe orientarse a que durante el análisis de riesgos el deseo de controlar amenazas sea mayor, incluyendo también aquellos activos que arrojen valoraciones diferentes a las críticas, esto es así, porque como ya fue reseñado se han visto casos en los que se invierte millones para mitigar o eliminar una amenaza crítica y resulta que ese riesgo que ni siquiera determinaron por su baja valoración se convierte en el peor dolor de cabeza de la compañía, incluso puede ser el agujero por el que se filtre un ataque que tire por la borda los millones invertidos en los otros riesgos.

Otra ventaja es que sea cuál sea la metodología de análisis de riesgo utilizada el equipo de seguridad tendrá un soporte sólido que le permitirá evidenciar ante la alta gerencia las nefastas consecuencias de aprobar planes de inversión insuficientes que no garantizan un control efectivo de las amenazas y por el contrario estos recursos limitados terminen siendo el primer enemigo de la gestión integral para la seguridad de la información y la mejora continua de la organización.

2.1.2 Beneficiarios

Dentro de los beneficiarios se encuentran:

- Todas las organizaciones tanto del sector público como privado.
- Los encargados de la seguridad informática de las compañías teniendo en cuenta que lo que se pretende es sensibilizar a la alta dirección de tener un mayor apetito a la hora de establecer controles aunque se tenga que subir un poco el presupuesto.

3. OBJETIVO GENERAL

Revisar la importancia de los resultados de un análisis de riesgos informáticos, para que los profesionales de la seguridad informática se concienticen que toda amenaza detectada debe ser controlada mediante el estudio de la metodología MAGERIT V.3, la norma ISO/IEC 27002:2013 y su aplicación en Latinoamérica.

3.1 OBJETIVOS ESPECÍFICOS

Analizar la metodología MAGERIT V.3 y la norma ISO/IEC 27002:2013.
Interpretar estadísticas sobre ataques de seguridad informática en Latinoamérica.
Revisar la importancia de controlar toda amenaza detectada por muy baja que parezca la afectación.

4. MARCO REFERENCIAL

Dentro del marco conceptual de este documento es necesario iniciar con la definición de monografía que presentada por Ander-Egg[19] "una monografía, en el sentido amplio del término, es una descripción, narración o exposición explicativa, sobre un tema concreto dentro de una ciencia, disciplina, tecnología o sobre un asunto en particular"; por tanto lo que se pretende en este caso en particular, es brindar un punto de vista, a partir de conceptos y explicaciones frente a la importancia de adoptar los controles para todas las vulnerabilidades que se evidencien o listen de un sistema informático, tras el informe emitido por una metodología de análisis del riesgo informático y, de este modo, proteger los activos de información, lo más permisible que se pueda.

Con la finalidad de llevar a cabo de manera estructurada cada una de las temáticas que le apuntan a los objetivos planteados de este escrito y con el ánimo de sumergir al lector desde un principio en las puntualidades del problema planteado, en el siguiente bloque, se revisaran los conceptos asociados a la seguridad de la información y la seguridad informática desde la perspectiva de un sistema de gestión de seguridad de la información.

4.1 MARCO CONCEPTUAL

4.1.1 Riesgo Informático

La Real Academia Española define el riesgo como aquella contingencia o proximidad de un daño[20], entonces si se asocia la posibilidad de que algo ocurra y el perjuicio que se puede sufrir con la seguridad informática, se estaría hablando de riesgo informático como toda vulnerabilidad o amenaza (física o lógica) que

[19] ANDER-EGG, Ezequiel. Cómo elaborar monografías, artículos científicos y otros textos expositivos. Madrid, 2017. 106p.

causa un daño al sistema (equipos o información) o lo que se conoce como activos informáticos.

4.1.2 Vulnerabilidad

Vulnerabilidad es todo punto débil de un sistema, ya sea por su diseño, implementación u operación, a través del cual se puede materializar una amenaza.

4.1.3 Amenaza

Es todo evento (humano, natural o técnico) que pueda afectar los activos de información (datos o infraestructura); cuando una amenaza se materializa se puede decir, que se está llevando a cabo un ataque informático y por ende una vulnerabilidad al sistema que, de no ser controlada, puede terminar con pérdida de información, daños, o interrupciones de servicio para la compañía.

4.1.4 Ataque Informático

Un ataque informático o ciberataque es cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información. [CESID:1997][21].

4.1.5 Integridad, Confidencialidad, Disponibilidad

Exponer al comienzo del marco conceptual las principales causas (ataque, riesgo, vulnerabilidad, amenaza) por las que hoy en día existe a nivel mundial

[20] RAE. Definición de Riesgo. https://dle.rae.es/?id=WT8tAMI
[21] Centro Superior de Información de la Defensa, “Glosario de Términos de Criptología”, Ministerio de Defensa, 3ª edición, 1997. Citado por Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 99

comunidades enfocadas en la seguridad informática brinda un contexto claro en lo que se busca al identificar riesgos y definir e implementar salvaguardas para resguardar cada uno de los activos informáticos de una compañía, pero ¿qué es lo que se realmente necesita proteger una organización? La respuesta es lo que se conoce como los principios de la seguridad de la información, Integridad, Disponibilidad y Confidencialidad los cuales fueron definidos en la norma ISO/IEC 13335-1 del 2004 de la siguiente manera:

Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos[22].

Disponibilidad: La propiedad de ser accesible y utilizable por una entidad autorizada[23].

Confidencialidad: La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados[24].

4.2 MARCO TEÓRICO

4.2.1 Vulnerabilidad, Amenaza y Ataque Informático

Dentro del marco conceptual se definieron, entre otros, los conceptos de vulnerabilidad, amenaza y ataque de forma clara y muy sucinta, en este bloque son vistos desde un enfoque 'organizacional' por llamarlo de otra forma, es decir que las empresas deben conocer cuáles son las vulnerabilidades para cada uno de sus activos informáticos y acto seguido identificar qué amenazas podrían

[22] GÓMEZ, L. y ÁLVAREZ, A. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, AENOR - Asociación Española de Normalización y Certificación, 2012.
[23] Ibíd., p. 35
[24] Ibíd., p. 35

explotar esas debilidades a través de un ataque informático, bien sea interno o externo.

Este ejercicio de identificación de vulnerabilidades y amenazas hace parte de la gestión del riesgo que engloba un sistema de gestión de seguridad de la información.

4.2.2 Sistema de Gestión de Seguridad de la Información – SGSI

> Uno de los principales activos que poseen las empresas es la información que manejan. Un correcto tratamiento de la información requiere la adopción de las medidas que sean necesarias para proteger los tres aspectos básicos de la misma: integridad, confidencialidad y disponibilidad. Un Sistema de Gestión de la Seguridad de la Información o SGSI sería, por tanto, un conjunto de medidas destinadas a preservar estos tres elementos de la información que maneja una empresa, independientemente del soporte, tipo, etc., de la misma. Para que estas medidas sean efectivas, deben llevarse a cabo a través de procesos estandarizados, documentados, conocidos y aplicados por toda la empresa[25].

La Organización Internacional de Normalización ISO y la Comisión Electrónica Internacional IEC utilizan el término SGSI para referirse a un Sistema de Gestión de la Seguridad de la Información que gracias a la cooperación y participación de muchos organismos desarrollan una serie de normas internacionales a través de diferentes comités técnicos; en lo que se refiere a seguridad informática fue elaborada la norma ISO/IEC 27001 como un modelo para crear, implementar, operar, supervisar, revisar y mejorar un SGSI.

Es importante saber que la ISO/IEC 27001 fue elaborada en el 2005 y que actualmente está vigente la primera y única revisión del año 2013 en la que influyeron dos aspectos importantes, primero el cumplimiento de la estructura de alto nivel conocida como “Anexo SL” para que tenga un aspecto similar a todos los

[25] GASCÓ, Ema. y Otros. Conceptos sobre seguridad informática. Madrid. 2013.

sistemas de gestión de la ISO y por otra parte se requería alinear la 27001 con la ISO 31000 de Gestión del Riesgo.

En todo caso un Sistema de Gestión de la Seguridad de la Información debe tener documentado unos Requisitos Generales, la Creación y Gestión del SGSI, su Implementación y Operación, así como la Supervisión y Revisión, aplicando Mantenimiento y Mejoras para que sea eficiente con el pasar del tiempo adaptándose a los cambios, que en materia tecnológica se vienen dando de forma acelerada, para de esta forma blindar a la organización de los diferentes riesgos y asegurar la cconfidencialidad, integridad y disponibilidad de sus activos de información.

4.2.3 Seguridad de la Información

La seguridad de la información se refiere a todas las medidas, mecanismos, estrategias y metodologías adoptados para proteger la integridad, confidencialidad y disponibilidad de la información. Entonces se protege con estos procedimientos los tres pilares de la seguridad de la información, los cuales son definidos por ESCRIBA[26] de la siguiente manera:

> **Integridad**: certificando que tanto la información como sus métodos de proceso son exactos y completos. **Confidencialidad**: asegurando que únicamente pueden acceder a la información y modificarla los usuarios autorizados. **Disponibilidad**: permitiendo que la información esté disponible cuando los usuarios la necesiten[27].

4.2.4 Seguridad de los Datos

Los datos han adquirido un lugar importante como recurso corporativo, pues en cierta medida, gran parte del éxito de muchas organizaciones esta asociados al

[26] ESCRIVÁ, G, ROMERO, R, y RAMADA, D. Seguridad informática. Madrid: Macmillan Iberia, S.A., 2013. p. 8
[27] Ibíd., p. 8

control y manejo que se les da a estos. Cuando se atenta contra la seguridad de los datos la capacidad de una compañía para seguir funcionado de manera normal se puede ver afectada[28].

4.2.5 Seguridad Informática

Inicialmente es posible definir la seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático[29]. En el mismo orden de ideas, la seguridad informática es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida[30]. También en función de lo que se quiere proteger, el mismo autor asocia la Seguridad Física a la protección física del sistema ante amenazas como inundaciones, incendios, robos, otros.

Mientras que la Seguridad Lógica se le llama a los mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos); dependiendo del lugar de la protección Cervera et all[31], clasifican la seguridad como Activa y Pasiva, la primera “se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas)”[32], mientras que la segunda “comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras)”[33].

---

[28] GUILLENSON, M. Administración de Bases de Datos. México. 2006. p. 271.
[29] UNIVERSIDAD DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme?. Valencia, 2016. Recuperado de https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/
[30] RAMOS, L.A. Seguridad Informática. España, 2014. p
[31] CERVERA, D. et al. Complementos de formación disciplinar. Tecnología. 2010.
[32] Ibíd.,. p. 1
[33] Ibíd.,. p. 1

4.2.6 Análisis de Riesgo Informático

En la actualidad las empresas son dependientes de la tecnología de la información, estas ayudan a la organización, en la realización de tareas de complejidad, lo que les rodea de riesgos o amenazas en el desenvolvimiento de las funciones de la misma.

En el mismo orden de ideas las empresas en la necesidad de organizar sus datos e interpretar los mismos, hacen uso del análisis de riesgo. Según la guía de gestión del riesgo[34], el análisis del riesgo es la primera parte de la seguridad informática, tiene como propósito establecer una probabilidad de ocurrencia de los riesgos como factor principal y el impacto sobre los datos informáticos.

Ahora bien la necesidad de un análisis de riesgo radica en una proyección, esta se realiza bajo datos pasados, seguros y un análisis de acontecimientos sucedidos bajo un esquema establecido. Este análisis permite el estudio de controles que ha establecido una empresa para proteger su información, donde puede ser encontrados fallos de seguridad, y donde se pone de manifiesto la vulnerabilidad de los sistemas de información.

Dicha labor es realizada por los actores de seguridad, los cuales entienden el proceso y tienen conocimiento acerca de las formas de mitigar amenazas. Esto causa que los gerentes manejen un presupuesto para la empresa y la protección de datos y activos.

Los activos son un valor para la empresas o bien una utilidad, tienen la particularidad de necesitar protección, lo cual radica en el aseguramiento de las

[34] COLOMBIA. MINTIC. Guía de administración del riesgo. Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

funciones de la organización, operaciones de negocio, permanencia de la empresa y logro de objetivos y metas trazadas.

Existen numerosos activos, clasificados[35] de la siguiente manera:

Activos de la información:

- Archivos de datos
- Bases de datos
- Documentos del sistema
- Manuales de operación
- Manuales de usuario
- Planes de continuidad y otros

Documentos impresos:

- Contratos
- Lineamientos
- Documentos de la empresa
- Resultados del negocio y otros

Activos de software:

- Software de aplicación
- Software de Sistema
- Herramientas de desarrollo

Activos físicos:

- Equipos de computo
- Equipos de comunicación
- Equipos técnicos en general

Personas:

- Personal
- Clientes

[35] ISO 17799. Código de práctica para la gestión de la seguridad de la información. 2005.

Servicios:

- Servicios de computación
- Servicios técnicos

Respecto a las amenazas, son conocidas como un perjuicio ocasionado, bien sea por un incidente deseado o no, cuando se ejecutan estas ponen en peligro la integridad, confidencialidad y la forma en cómo se encuentra disponible el activo.

La amenaza puede ser deliberada; cuando ya fueron planificadas y tienen finalidad de daño, también pueden ser accidentales cuando no se tiene la intención de causar daño sobre el activo.

Asimismo, cuando se habla de valorización de amenazas[36] y su afectación, se estima la frecuencia con que las mismas suceden, teniendo la probabilidad de ocurrencia (la tasa anual de ocurrencia) y el porcentaje de degradación (el daño que se causa por un incidente).

4.2.7 Gestión del Riesgo Informático

> El análisis de riesgos permite determinar cómo es, cuánto vale y cuan protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos[37].

El análisis de riesgos informáticos es un insumo clave al momento de implementar medidas de protección sobre los activos de información de una organización; lo

[36] FERRERO, Eduardo. Análisis y gestión de riesgos en iMat del sistema de información de I.C.A.I. Tesis Universidad Pontificia Comillas Escuela Técnica Superior de Ingeniería (ICAI), Madrid, Junio del 2006, p. 140.

que hacemos después con este informe y plan de tratamiento de riesgos es realmente un tema interesante y de gran interés para el área de la seguridad informática, en el entendido que las compañías invierten fuertes sumas de dinero para proteger su información.

La importancia de conocer los riesgos informáticos a que está expuesta una compañía, así como determinar los controles adecuados para cada uno de estos es fundamental para la continuidad del negocio y las grandes empresas lo saben, por eso existen diferentes estándares y metodologías de análisis y gestión del riesgo informático, entre las que se destacan Cobit, ISO 27001 y Magerit.

Igual que en otras áreas, estas guías buscan eliminar, minimizar o transferir el riesgo. El objetivo principal de la gestión del riesgo informático es, a entender del autor, identificar cada uno de los riesgos que pueden ocasionar daños (físicos o intangibles) cuantificando el impacto económico sobre los activos, para de esta forma establecer los controles adecuados para cada situación y proteger así el sistema; por ejemplo, el sistema operativo Windows, para protegerse posee un firewall basado en host que permite crear filtros para conexiones entrantes y salientes del servidor, creando diferentes perfiles que se puedan aplicar según la categoría del equipo (red interna, VPN, servidores)[38].

Como la guía Magerit y la norma ISO 27001 son de las más utilizadas actualmente, se procede a su análisis en un capítulo aparte para describir sus bondades frente al panorama actual de la seguridad informática y de este modo, comprender el propósito de esta monografía.

---

[37] ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 10

[38] GOMEZ, J. Seguridad en sistemas operativos Windows y GNU/Linux. Bogotá. Firewall de Windows. Bogotá, 2012.

4.3 MARCO LEGAL

4.3.1 Convenio de Budapest y otras Normas Internacionales

En noviembre del 2001 en Hungría fue adoptado por Canadá, Japón, Estados Unidos y Sudáfrica el Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC conocido como el Convenio de Budapest, considerado por muchos como el primer tratado internacional como medida para los delitos informáticos y el 1º de junio del 2004 entró en vigor y a partir de esta fecha muchos países han firmado y ratificado su adhesión.

Entre los países Latinoamericanos adheridos a este convenio se encuentran México, El Salvador, Argentina, Costa Rica, Uruguay, Chile, República Dominicana, Panamá, Perú y Colombia.

De manera sencilla se puede determinar que el principal objetivo de este convenio es adoptar una legislación que permita facilitar y orientar en la prevención de conductas delictivas en temas informáticos y provea herramientas penales eficientes que permitan detectar, investigar y sancionar conductas antijurídicas.

El Consejo Europeo consideró que los delitos cibernéticos requieren una política penal común como medida preventiva en el ciberespacio adoptando una legislación apropiada y con el fortalecimiento de la cooperación internacional.

Otras normas internacionales que le apuntan a la seguridad informática pueden apreciarse en la Tabla 1, a continuación:

Tabla 1. Otras normas internacionales en seguridad informática

NORMA	RESUMEN
Resolución AG/RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos.	Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Estipula tres vías de acción: ☐ Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores - CSIRT. Este cometido fue asignado al Comité Interamericano Contra el Terrorismo - CICTE. ☐ Identificación y adopción de normas técnicas para una arquitectura segura de Internet. Esta labor es desarrollada por la Comisión Interamericana de Telecomunicaciones. ☐ Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.
Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 2004.	Por la cual se establecen los lineamientos de la Política de Seguridad Externa Común Andina. Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.
Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" Asamblea General de las Naciones Unidas. (2009)	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información

Fuente: Documento Conpes 3701, Lineamientos de Política para Ciberseguridad y Ciberdefensa, Republica de Colombia, Bogotá D.C., 14 de julio de 2011

4.3.2 Normas de Seguridad Informática en Latinoamérica

Los avances tecnológicos en materia de hardware, software e internet vienen sorprendiendo al mundo día tras día, esto es algo que productores y usuarios saben porque genera ingresos y facilita muchas tareas; lo que no se mueve al mismo rito de los avances son las normas y los mecanismos jurídicos y legales que permitan demostrar, procesar y judicializar un siniestro informático.

Si bien el Convenio de Budapest brinda un lineamiento general y de mutua colaboración entre varios países, no todos lo han adoptado y algunos lo hacen pero se quedan cortos en la definición de un marco institucional y en las capacidades técnicas que se requieren. En Latinoamérica, por ejemplo, México, El Salvador, Argentina, Costa Rica, Uruguay, Chile, República Dominicana, Panamá, Perú y Colombia han firmado el Convenio e implementado algunas normas que se detallan en la Tabla 2, a continuación:

Tabla 2. Normas de Cyberseguridad en Latinoamérica

PAIS	NORMAS
Argentina	Ley Nº 26.388 del año 2008. Que incorpora en su ordenamiento jurídico una serie de delitos informáticos.
Uruguay	Aprobó la Ley de Protección de Datos Personales y Acción de Habeas Data N° 18.331 el 11 de agosto de 2008.
Paraguay	Ley 4439 del 2011, modifica y amplia varios artículos de la ley n° 1160/97 código penal.
Chile	Ley relativa a delitos informáticos No.19223 de 1993, actualmente cursa un proyecto de ley para modificar e incorporar nuevas formas de comisión por los avances tecnológicos recientes.
Bolivia	Ley n° 1768 de 1997 modificaciones al código penal sobre Delitos Informáticos.
Brasil	Ley 12.737 del 2012 tipificación criminal de los delitos informáticos y

	otras providencias.
Ecuador	Ley de comercio electrónico, firmas electrónicas y mensajes de datos No. 2002-67.
Perú	Ley de Delitos Informáticos que incorpora dos artículos al código penal mediante el Decreto Legislativo Nº. 635 de 1999.
Venezuela	En septiembre del 2001 se firma en Caracas la Ley especial contra delitos informáticos.
México	Código Penal Federal (Reformas 17 de mayo de 1999) Persona física o moral del sector privado (Art. 211 Bis 1) Servidor público del Estado (Arts. 211 Bis 2 y 3)
Colombia	Revisar Capitulo 4.3.3 Colombia Ley 1273 de 2009 y el Código de Ética.
Panamá	Aunque está adherido al convenio de Budapest desde el 2014, el Código penal solo tipifica 2 conductas como delitos informáticos.
Republica Dominicana	Ley Nº 53-07 del 2007 Ley Especial contra Crímenes y Delitos de Alta Tecnología.
El Salvador	Ley 260 Especial de Delitos Informáticos y Conexos, aprobada el 4 de febrero del año 2016 para proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las TIC.
Costa Rica	Ley 9048 del 2012 Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal.
Puerto Rico	Código Penal y la ley 1165 del 2008 o ley de espionaje cibernético.

Fuente: El Autor

4.3.3 Seguridad Informática en Colombia Ley 1273 de 2009

Así como sucede en otros países, en Colombia la tecnología de la información nos brinda muchas facilidades en diferentes aspectos de nuestra cotidianidad; como

son: transacciones financieras y comerciales, procesos mecánicos, industriales y laborales, interacción a través de redes sociales, en fin, estamos procesando información a través de dispositivos que pueden ser víctimas de ataques informáticos y que pueden afectar nuestra vida personal y laboral.

El 11 de septiembre de 2013, Colombia recibe su invitación del Consejo de Europa para que se adhiera al Convenio de Budapest y lo materializo 5 años después mediante la aprobación del proyecto de ley 1928 del 2018, para resumir la aproximación de esta ley se puede precisar que los 48 artículos del convenio de Budapest están acogidos en Colombia en diferentes normas, como por ejemplo, la Ley 1273 de 2009 (de la protección de la información y de los datos.), la Ley 1581 de 2012 (protección de datos, divulgación y denuncia de las violaciones de seguridad), la Ley 527 de 1999 ("…acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales…") y otras normas, así como los Conpes 3701 de 2011 (lineamientos de política de ciberseguridad y ciberdefensa) y 3854 de 2016 (seguridad digital integral).

La Ley 1273 de 2009 "De la Protección de la Información y los Datos"[39] es a entender del autor, la principal herramienta jurídica que el estado ha dispuesto para la judicialización de los delitos informáticos comúnmente tipificados a nivel mundial, y que en el caso de Colombia está alineado al articulado del convenio de Budapest.

La ley 1273 del 2009 lo que hace es clasificar los delitos informáticos con el fin de penalizar a los infractores, creando nuevos tipos penales en el código penal para castigar los delitos informáticos y la protección de la información y de los datos con prisión de hasta 120 meses y multas que llegan a los 1500 salarios mínimos legales mensuales vigentes.

[39] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 de 2009: Capítulo I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

En este sentido la Ley 1273 en el Capítulo I "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"[40] tipificó las siguientes violaciones:

1. Acceso abusivo a un sistema informático.
2. Obstaculización ilegítima de sistema informático o red de telecomunicación.
3. Interceptación de datos informáticos.
4. Daño Informático.
5. Uso de software malicioso.
6. Violación de datos personales.
7. Suplantación de sitios web para capturar datos personales.

Algo a resaltar de esta norma son las circunstancias de agravación punitivas, las cuales determinan que las penas para los delitos tipificados en el párrafo anterior se aumentarán, de la mitad a las tres cuartas partes, si la violación se hace sobre redes o sistemas del estado o entidades financieras, si son cometidas por servidores públicos, por aprovecharse de la confianza del dueño de la información, obteniendo provecho para sí mismo o por actos terroristas que pongan en riesgo la seguridad nacional.

El segundo capítulo denominado "De los atentados informáticos y otras infracciones" enfatiza en las siguientes actuaciones:

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

[40] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 de 2009, op. cit, p. 1

5. ANALIZAR LA METODOLOGÍA MAGERIT V.3 Y LA NORMA ISO/IEC 27002:2013

5.1 MAGERIT V3

La metodología de análisis y gestión de riesgos Magerit de acuerdo con sus creadores, el Consejo Superior de Administración Electrónica de Madrid,

> Surge como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. El uso de TIC's supone beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios[41].

Magerit tuvo su primera aparición en 1997 y estaba más que todo orientada a los riesgos fundamentales de los sistemas de información; en el 2005 se llevo a cabo su primera revisión en la cual profundizó un poco más e incorporó la gestión del riesgo; actualmente está vigente la versión 3.0 soportada en tres libros, 1 método, 2 catalogo de elementos y 3 guía técnica, en los que se puede notar que el Consejo Superior de Administración Electrónica de Madrid tuvo en cuenta la evolución de las normas internacionales de la Organización Internacional de Normalización ISO.

Magerit apunta directamente a los siguientes objetivos:

> "Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC). Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control. Y Preparar a la Organización para

[41] ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 6

> procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso[42]"

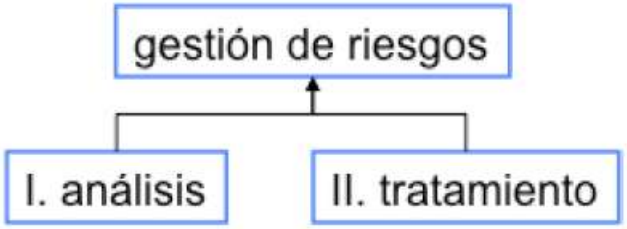
Al revisar con detenimiento, el primer objetivo de esta metodología es claro y directo para generar conciencia en los 'Responsables' de las organizaciones, refiriéndose no solo a los ingenieros y personal de seguridad, sino que también abarca a directivos, accionistas y todos los altos mandos, porque no es solo manipular información personal y de todo tipo de datos, sino velar por el buen uso de esta, igual que la custodia de los activos físicos y la continuidad del negocio.

Como conjunto Magerit realiza 2 tareas fundamentales:

> Análisis de riesgos, que permite determinar qué tiene la organización y estimar lo que podría pasar; y el Tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones[43].

Estas 2 actividades se combinan en el proceso denominado Gestión de Riesgos.

Figura 1. Gestión de riesgos



Fuente: Magerit – Libro 1

Esta concepción de Magerit de defender para controlar lo malo, pero estar siempre listos para dar respuesta oportuna a un incidente es otra de las premisas

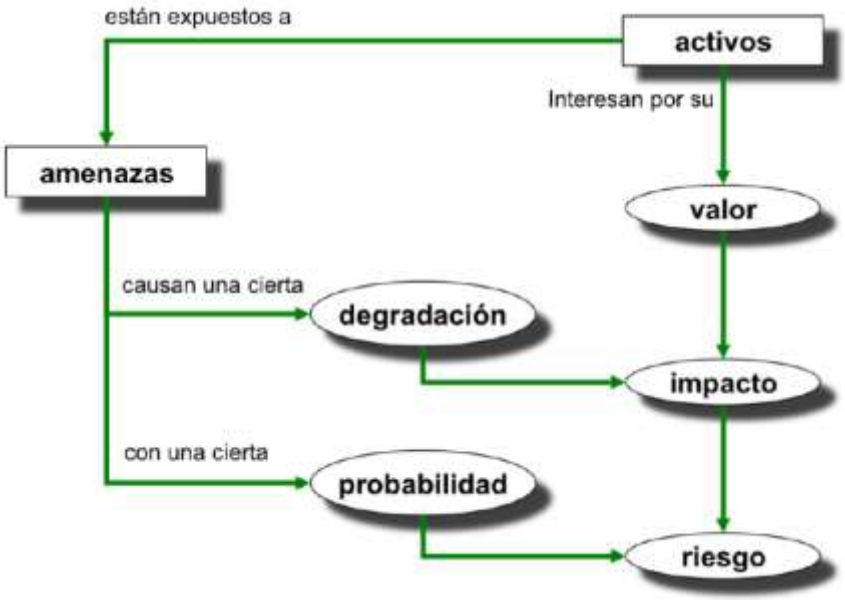
[42] ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 8
[43] Ibíd., p. 19

fundamentales que todo profesional de TIC y en especial aquellos que lideran la seguridad deben tener grabada en su día a día para que se mentalicen que no hay que dejar un solo punto sin vigilar.

5.1.1 Análisis de Riesgos

El análisis de riesgos de Magerit considera los Activos, Amenazas y salvaguardas, para estimar el impacto y el riesgo. Este proceso no es tan sencillo, aunque la guía es muy clara requiere de mucha dinámica y participación de muchos actores, gerenciales, técnicos y asistenciales para obtener de ellos la más preciada y detallada información, pues este será el punto de partida para saber el estado de la organización y tomar las mejores decisiones en la etapa de gestión de riesgos. En la figura 2 se puede apreciar la ruta que sigue la guía para determinar el riesgo:

Figura 2. Ruta para el análisis de riesgos potenciales



Fuente: Magerit – Libro 1

La guía Magerit V3[44] propone que el Método de Análisis de Riesgos – MAR se lleve a cabo por medio de las tareas:

MAR.1: Caracterización de los activos: busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia. Esta actividad finaliza con el informe "modelo de valor"[45].

MAR.2: Caracterización de las amenazas: busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación)[46]. MAR.2 concluye con el informe mapa de riesgos.

MAR.3: Caracterización de las salvaguardas: esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar[47].

MAR.4: Estimación del estado de riesgo: esta actividad realiza un informe del estado de riesgo (estimación de impacto y riesgo) y un informe de insuficiencias (deficiencias o debilidades en el sistema de salvaguardas)[48]

Es necesario precisar que las valoraciones realizadas en MAR 1 son teóricas y basadas en la percepción de las personas involucradas en este proceso, pero una vez se obtiene un panorama más amplio con la caracterización de amenazas y

[44] ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 36.
[45] Ibíd.,. P. 36
[46] Ibíd.,. P. 36
[47] Ibíd.,. P. 36
[48] Ibíd.,. P. 37

salvaguardas del MAR 2 y 3 las estimaciones de impacto y riesgo toman valores más reales y apropiados para los informes de MAR 4. En la figura 3 podemos comprender los cuatro pasos del método de análisis de riesgo de Magerit.

Figura 3. Método de análisis de riesgo de Magerit

Fuente: TiThink, Gestión de Riesgos Magerit

Para explicar brevemente los procesos que realiza Magerit y comprender mejor el esquema anterior, las amenazas son todas aquellas acciones o cuestiones de origen natural o del entorno, técnicas o tecnológicas, accidentales o intencionales que pueden ocurrir y causar daño a los activos de la organización, pero este perjuicio sobre el activo se valora por Degradación y Probabilidad; el primero estima cuanto se pierde en el valor del activo y el segundo tiene en cuenta que tan probable o improbable puede darse la amenaza. Entonces conociendo el valor del activo y la degradación que ocasionan las amenazas se obtiene el Impacto, y con este último y la probabilidad obtenida se determina el Riesgo, que en esta parte de la guía se conoce como Riesgo Potencial.

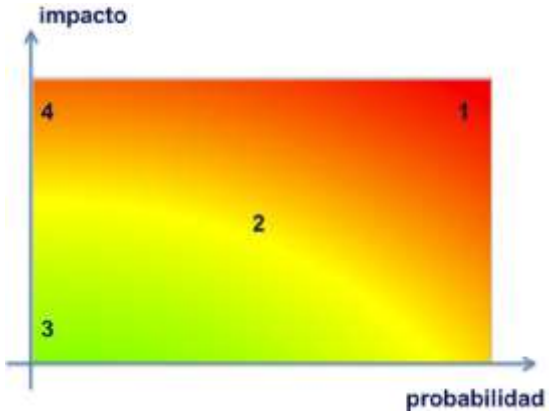
El riesgo crece de acuerdo al impacto y la probabilidad y de esta forma se obtienen zonas de riesgo que nos indican o clasifican de mayor a menor importancia los riesgos.

Tabla 3. Zonas de Riesgo

ZONA	TIPO RIESGO
1	Riesgos muy probables y de muy alto impacto.
2	Franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
3	Riesgos improbables y de bajo impacto.
4	Riesgos improbables pero de muy alto impacto.

Fuente: Magerit Libro 1, P. 29 - 30

Figura 4. Método de análisis de riesgo de Magerit



Fuente: Magerit Libro 1, P.30

La valoración del activo debe realizarse pensando en su protección, es decir si el activo es importante requerirá de mayor seguridad, para esta guía existen activos denominados esenciales por la información que poseen y los servicios que prestan, los demás activos son dependientes o subordinados de los primeros y

constituyen arboles de dependencia; en todo caso la valoración puede ser cualitativa o cuantitativa y consiste en determinar el costo que supondría recuperarse de cualquier acción que destrozase el activo.

Un aspecto importante de Magerit en lo referente a la valoración es que además de las que denomina Dimensiones Básicas (confidencialidad, integridad y disponibilidad) considera útil valorar en los activos esenciales la autenticidad y trazabilidad de servicios y datos.

Magerit define “las salvaguardas, o contra medidas, como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo”[49] y proporciona en el libro 2 Catalogo de Elementos una relación de salvaguardas adecuadas para cada tipo de activo y la medición de estas se realiza desde dos perspectivas, eficacia frente al riesgo y por su madurez o tipo de protección.

Tabla 4. Tipos de Salvaguarda

EFECTO	TIPO
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: Magerit Libro 1, P. 29 - 34

[49] ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – V 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 31.

Tabla 5. Eficacia y Madurez de la Salvaguarda

FACTOR	NIVEL	SIGNIFICADO
0%	**L0**	Inexistente
	L0	Inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
100%	**L5**	Optimizado

Fuente: Magerit Libro 1, P. 29 - 34

En este punto, volviendo la mirada a la figura 3. Método de análisis de riesgo de Magerit, sobre las salvaguardas una vez desplegadas se repite el cálculo del impacto, ahora teniendo en cuenta el nuevo nivel de degradación obteniendo lo que se conoce como impacto residual, lo mismo ocurre con los riesgos, se repite la formula usando el impacto residual y la probabilidad residual obteniendo el riesgo residual.

5.1.2 Tratamiento del Riesgo

Una vez que la organización ha desarrollado un análisis de riesgo y obtenido una información valiosa en cuanto al panorama de los impactos y riesgos a los que se encuentra expuesto el sistema llega el momento de tomar decisiones respecto a cada una de las consideraciones y obligaciones que se desprendan, bien sea de orden legal o de naturaleza intangible (reputación, relaciones internas y externas, etc.), en todo caso Magerit sugiere una calificación del riesgo así:

1. Es **crítico** en el sentido de que requiere atención urgente. 2. Es **grave** en el sentido de que requiere atención. 3. Es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento. 4. Es **asumible** en el sentido de que no se van a tomar acciones para atajarlo[50].

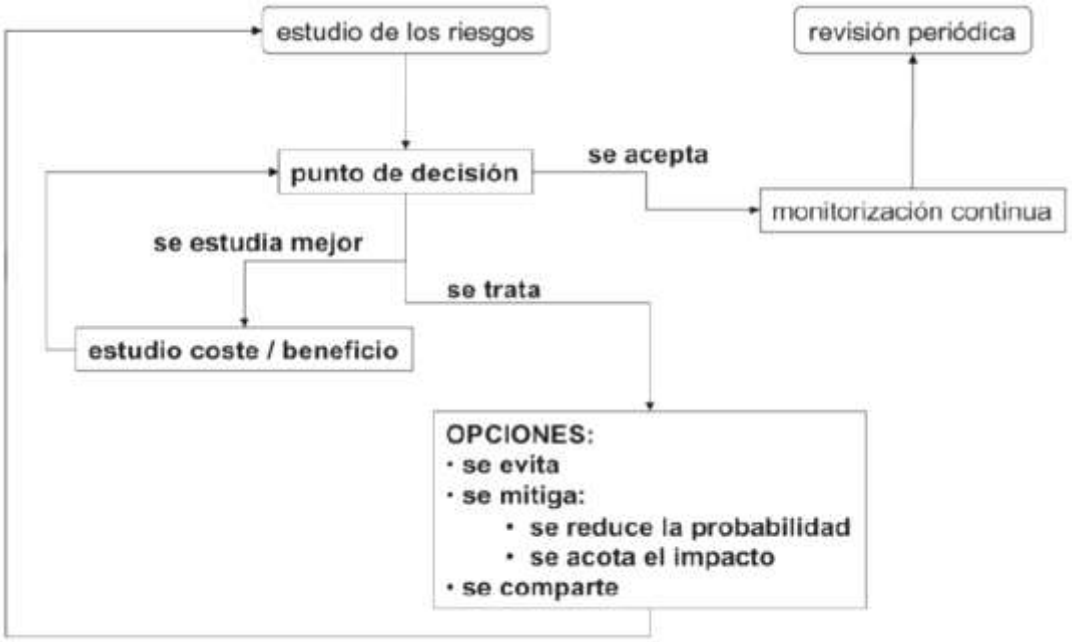
La aceptación del riesgo que implica la opción 4, es de acuerdo a la guía Magerit[51] arriesgada y debe tomarse con prudencia y justificación, por ejemplo cuando el impacto residual es asumible, o el riesgo residual es asumible ó cuando el coste de las salvaguardas es desproporcionado en comparación al impacto y riesgo residuales.

Como quiera que sea a partir de estas calificaciones sobre los riesgos se desarrollaran las acciones directas para proteger el sistema y es importante tener plena conciencia de la realidad actual en el mundo de la ciberdelincuencia y su evolución en las técnicas de ataque y el crecimiento de estos actores que mas que retos y reconocimiento hoy tienen claro que pueden obtener mucho dinero en este medio.

Como el tratamiento de riesgos trata de decisiones y tareas lo primero que deben hacer los órganos de gobierno de una compañía es, primero evaluación y como segundo paso el tratamiento. En la Figura 6 a continuación, Magerit resume las decisiones que pueden tomarse después de haber estudiado los riesgos.

Figura 5. Decisiones de tratamiento de los riesgos

[50] MAGERIT LIBRO 1, op. cit, p. 47
[51] Ibíd., p. 47



Fuente: Magerit Libro 1, P.47

Dentro del proceso de evaluación si el valor residual es igual al valor potencial se entiende que las salvaguardas existentes no son exitosas, aquí se debe acompañar cada cifra residual de lo que se debería hacer y no se ha hecho en un documento llamado informe de insuficiencias para que los altos mandos tengan la mayor claridad posible al momento de tomar decisiones. Este es otro punto de referencia que los encargados de la seguridad informática deben afianzar y reforzar buscando que los responsables de decidir no titubeen y dejen de aplicar medidas que son o serán necesarias.

Para el tratamiento del riesgo la guía Magerit 3.0 sugiere dos opciones a la dirección: Reducir el riesgo residual aceptando un menor riesgo o Ampliar el riesgo residual aceptando un mayor riesgo.

> En condiciones de riesgo residual extremo, casi la única opción es reducir el riesgo. En condiciones de riesgo residual aceptable, podemos optar entre aceptar el nivel actual o ampliar el riesgo asumido. En cualquier caso hay que mantener una

> monitorización continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y se reaccione ante cualquier desviación significativa. En condiciones de **riesgo residual medio**, podemos observar otras características como las pérdidas y ganancias que pueden verse afectadas por el escenario presente, o incluso analizar el estado del sector en el que operamos para compararnos con la "norma". [52].

La incertidumbre del análisis (sospechas u otro tipo que pueda afectar al impacto o la probabilidad) también existe y Magerit es claro al señalar que toda incertidumbre se debe considerar mala y se debe hacer algo al respecto.

5.1.3 Eliminar, Mitigar, Compartir o Financiar el Riesgo

Eliminar es una opción frente a un riesgo que no es aceptable, es decir si tenemos dentro de nuestro sistemas elementos que apartándolos no afecten significativamente podemos prescindir de ellos, por su parte los activos esenciales como información y servicios son casi que intocables para esta opción. Al optar por eliminar fuentes de riesgo conlleva a realizar un nuevo análisis de riesgos sobre el sistema modificado.

Mitigar el riesgo es tomar una de dos opciones: Reducir la degradación causada por una amenaza, o Reducir la probabilidad de que una amenaza se materialice.
Sea cual sea la decisión lo que se debe hacer es mejorar las salvaguardas y esto muchas veces sugiere incorporar nuevo equipamiento que de paso viene acompañado de sus propias amenazas, así que se debe repetir el análisis de riesgos y validar si con esta mejora el riesgo es menor que el del sistema original.

Compartir el riesgo brinda dos métodos: El Riesgo Cualitativo externalizando componentes del sistema, de forma que se reparten responsabilidades; y El Riesgo Cuantitativo contratando seguros y el asegurador responde por las

[52] ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – V 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 49.

consecuencias (en caso de ocurrencia) a cambio de una prima. También se debe repetir el análisis del sistema resultante al compartir el riesgo.

Financiar el riesgo es la opción que toma la alta dirección cuando simplemente acepta un riesgo por lo que deberían reservar fondos (de contingencia) o adquirir pólizas en caso que se materialice el riesgo y se deba afrontar sus consecuencias. Esta opción generalmente no modifica el sistema, así que no se deberá repetir el análisis de riesgo.

5.2 GUÍA ISO-IEC 27002 DOMINIOS, CONTROLES Y OBJETIVOS

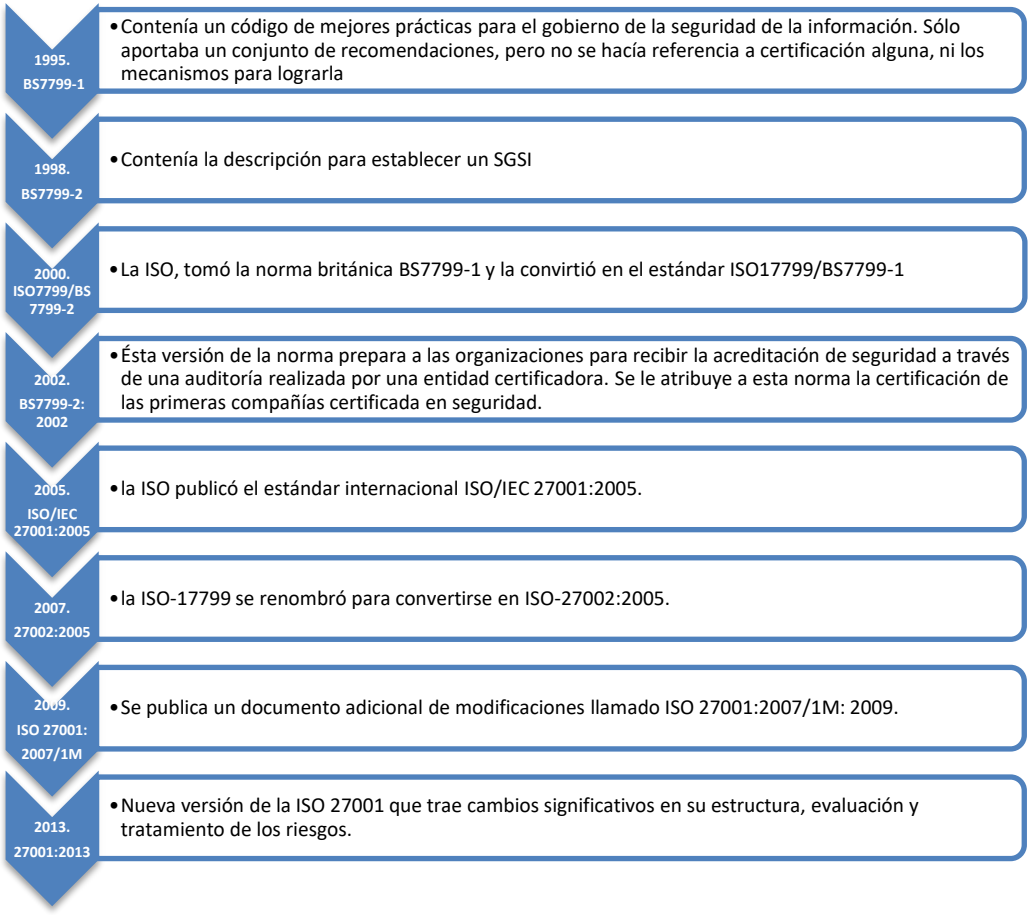
5.2.1 Estándar ISO/IEC 27000 Evolución y Estructura

En el libro Seguridad informática, ESCRIVÁ y Otros[53]. dice: para gestionar de forma adecuada la seguridad de la información se han desarrollado un conjunto de estándares que se han convertido en el marco para establecer, implantar, gestionar y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) refiriéndose a la norma ISO/IEC 27000 un conjunto de estándares definidos por la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission), que enmarcan la gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El origen y la evolución de la norma ISO/IEC 27001:2013 puede comprenderse de manera concreta e ilustrativa en la Figura 6., a continuación.

Figura 6. Evolución de la Norma ISO/IEC 27001:2013

[53] ESCRIVÁ, G, ROMERO, R, y RAMADA, D. Seguridad informática. Madrid: Macmillan Iberia, S.A., 2013. p. 7



Fuente: El Autor

La ISO/IEC 27001 de 2013 es la que orienta esta serie y define los requisitos del sistema de gestión de seguridad de la información y es la norma con la que son certificados los SGSI de cualquier compañía por auditores externos. Agrupa en su anexo A, los dominios, objetivos de control y controles que desarrolló la ISO 27002:2005, para que las organizaciones los apliquen como contramedidas a los riesgos y amenazas detectados en la etapa de análisis y gestión de riesgos durante el desarrollo de sus SGSI.

La estructura de la norma ISO/IEC 27001:2013 comprende dos partes, la primera se resume en la Figura 7., en este bloque se encuentra la introducción y los diez puntos que a continuación reseñados:

Figura 7. Estructura de la Norma ISO/IEC 27001:2013

Fuente: El Autor

1. Objeto y campo de aplicación: Presenta su finalidad y alcance.
2. Referencias normativas. Cual o cuales normas se utilizan.
3. Términos y definiciones: Basados en la ISO/IEC 27000.
4. Contexto de la organización: Requiere determinar necesidades y expectativas dentro y fuera de la organización que afecten al SGSI.
5. Liderazgo: La importancia de la alta dirección y su compromiso con el SGSI, y asignándoles tareas vitales como establecer políticas, asignación de los recursos necesarios para su implementación y operatividad.
6. Planificación: Valoración, análisis y evaluación de los riesgos informáticos y el tratamiento de estos.
7. Soporte: Definir la importancia de los recursos de la organización, las partes interesadas, las comunicaciones y la información documentada.
8. Operación: Se establece la planificación y el control de la operación.
9. Evaluación de desempeño: Definir acciones de seguimiento, medición, análisis y evaluación del SGSI.
10. Mejora: Ejecutar el seguimiento, medición, análisis y evaluación del SGSI.

La segunda parte de la norma ISO/IEC 27001:2013 comprende el Anexo A (ISO/IEC 27002) correspondiente a la guía de buenas prácticas de seguridad de la información y por ser parte fundamental del presente escrito es explicado con mayor detalle en el siguiente apartado.

5.2.2 ISO/IEC 27002 Dominios, Objetivos y Controles

Esta guía se publicó en Julio del 2007, actualizando lo que fue ISO 17799:2005; es una guía de buenas prácticas incorporada dentro de la serie 27000 como el Anexo A y donde se encuentran los dominios, objetivos de control y controles que se recomiendan para mejorar o asegurar los activos de información. No es certificable y su anterior versión contenía 39 objetivos de control y 133 controles, agrupados en 11 dominios. Actualmente son 114 controles de la ISO/IEC 27002:2013 que apuntan a 35 objetivos y están agrupados por los 14 dominios descritos en la Figura 8., a continuación: siguientes:

Figura 8. Dominios de Control ISO/IEC 27002:2013

Fuente: El Autor

Dentro de los dominios se especifican los objetivos de cada uno de los controles para la seguridad de la información y para cada control se indica una guía para su implantación. En total son 114 controles apuntando a 35 objetivos, pero cada organización debe considerar previamente cuáles aplica de acuerdo a sus necesidades y posibilidades, de igual modo las compañías pueden aportar controles o medidas adicionales que sean evaluadas. Algo importante aclarar es que no se trata solo de prescindir de algunos controles, se debe justificar claramente la no incorporación de estos.

Los controles del anexo A de la norma ISO/IEC 27001:2013 agrupados por dominios y objetivos se presentan de manera explicativa en la sección de anexos al final de este documento.

Al tener pleno conocimiento de los 114 controles que dispone la guía de buenas prácticas, es preciso aclarar que la determinación de estos es un proceso que debe desarrollarse con cautela y la mayor precisión requerida teniendo en cuenta que estas acciones son pensadas y determinadas para reducir la probabilidad y el impacto de la materialización de los riesgos, además esta etapa debe estar en constante revisión y actualización.

5.2.3 Declaración de Aplicabilidad (SOA)

La Declaración de Aplicabilidad, SOA por sus siglas en ingles (Statement of Applicability) es un documento requerido por la norma ISO/IEC2 27001 en el que se listan los objetivos y controles que serán implementados y tal como se manifestó en el titulo anterior, también deben quedar establecidas las justificaciones de los controles que no serán tenidos en cuenta. El SOA es tan esencial para un sistema de gestión de seguridad de la información que normalmente se realiza un análisis de brechas (GAP Analysis) con el cual se crea

un panorama que identifica riesgos, controles, requisitos legales, contractuales, etc., para marcar la diferencia entre lo que la compañía debería implementar y lo que realmente dispone. La declaración de aplicabilidad debe estar bajo revisión y actualización constante.

5.2.4 Ventajas y Desventajas de la Norma ISO/IEC 27001

Las principales ventajas de trabajar con base a esta norma son:

- Es aplicable a cualquier tipo de empresa, pública o privada, de tamaño grande, mediana o pequeña.
- Permite a las organizaciones establecer directrices claras y principios para implementar, mantener y mejorar su gestión frente a las amenazas y riesgos informáticos.
- Gracias a la identificación de activos brinda mayor control sobre estos.
- Reduce y/o controla riesgos gracias a la implementación de políticas y procedimientos de seguridad.
- Genera responsabilidad en los altos mandos y conciencia sobre la seguridad de la información a todos los empleados.
- Promueve el cumplimiento de la legislación y reglamentación vigente.
- Invita a la mejora continua, ya que permite identificar y corregir debilidades.
- También genera confianza en clientes y proveedores que tienen en cuenta una certificación de este tipo.

Hablar sobre desventajas con una norma técnica internacional revisada por muchos expertos y con la experiencia de la ISO en este campo, no es una tarea fácil, ya que no es lo mismo una compañía bien organizada y con procedimientos claros y definidos a una empresa indiferente a unas políticas de seguridad que

protejan sus activos de información, sin embargo algunos contras que se pueden identificar sobre esta norma son:

- Su implementación suele resultar costosa, sobre todo para pequeñas empresas.

- No existe una descripción detallada a la hora de identificar los riesgos.

- Algunos requisitos son difíciles de interpretar y de entender por directivos poco dados a la seguridad informática.

6. ATAQUES DE SEGURIDAD INFORMÁTICA EN LATINOAMÉRICA.

Entre 2016 y 2017 la mitad de los virus detectados en América Latina estaban asociados a la categoría de troyanos. En mayo de 2017 se sufrió el ataque de *WannaCry*, el más grande ataque de un virus informático en la historia, dirigido a diversas instituciones y empresas de más de 100 países; se conoció que los atacantes obtuvieron ganancias estimadas en 100.000 dólares aproximadamente, pero de acuerdo a información de la empresa Rusa Kaspersky[54], los daños ocasionados superaron ampliamente la cifra en los usuarios afectados.

Por su parte ESET Security[55] reveló que una de cada dos empresas en Latinoamérica ha sido objeto de malware en el último año, y cerca de un 46,7% las compañías en Colombia sufrieron algún tipo de incidente relacionado con seguridad informática.

Al igual que Kaspersky el estudio de ESET señala que el ransomware, código malicioso que se dedica a secuestrar información digital, se posicionó en el segundo lugar de incidentes, con un 16% desplazando al phishing hacia la tercera posición con un 15%[56].

Desafortunadamente ante estos ataques, la mayoría de las compañías optan por pagar la suma solicitada por los ciberdelincuentes en vez de tomar medidas de seguridad; para Camilo Gutiérrez, jefe de Laboratorio de Investigación de ESET Latinoamérica la principal solución que están encontrando las empresas para este tipo de amenazas es el pago, y cuando se paga, se promueve el éxito de este tipo de amenazas[57].

[54] KASPERSKY. Cifras reveladas por la compañía de seguridad informática Kaspersky durante la séptima Cumbre Latinoamericana de Analistas de Seguridad en septiembre del 2017
[55] ESET. Eset Security Report 2017.
[56] Ibíd., p. 1

Los datos del reporte de Kaspersky también indican que:

> El 56% de los entrevistados (4.000 profesionales) la mayor preocupación en materia de seguridad son precisamente códigos maliciosos, seguido por el 52% que dijo estar preocupado por las vulnerabilidades de software y de sistemas y el tercer puesto, con el 27% lo ocupa el phishing, siendo Trojan-Ransom el de crecimiento más acelerado[58].

Al volcar la mirada al sector bancario el panorama es igual de crítico o un poco mayor a otros sectores; es así como de acuerdo con el reporte "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe", de la Organización de los Estados Americanos (OEA) presentado en septiembre de 2018 señala los siguientes hallazgos:

> "- al menos 9 de cada 10 entidades bancarias sufrieron incidentes cibernéticos en el último año. - el 37% de los bancos de la Región fueron víctimas de ataques que resultaron efectivos. - el 39% de los incidentes no son reportados, dato que en el caso de las entidades bancarias de mayor tamaño baja hasta el 19%. - 6 de cada 10 usuarios que no utilizan servicios de banca digitales lo hace por desconfianza sobre la seguridad de las transacciones."[59]

6.1 Delitos informáticos en Latinoamérica

A continuación se revisa el panorama de los delitos y ataques informáticos más habituales en algunos países latinoamericanos, como Brasil, Argentina, Colombia, México y El Salvador:

6.1.1 Delitos más comunes en Colombia

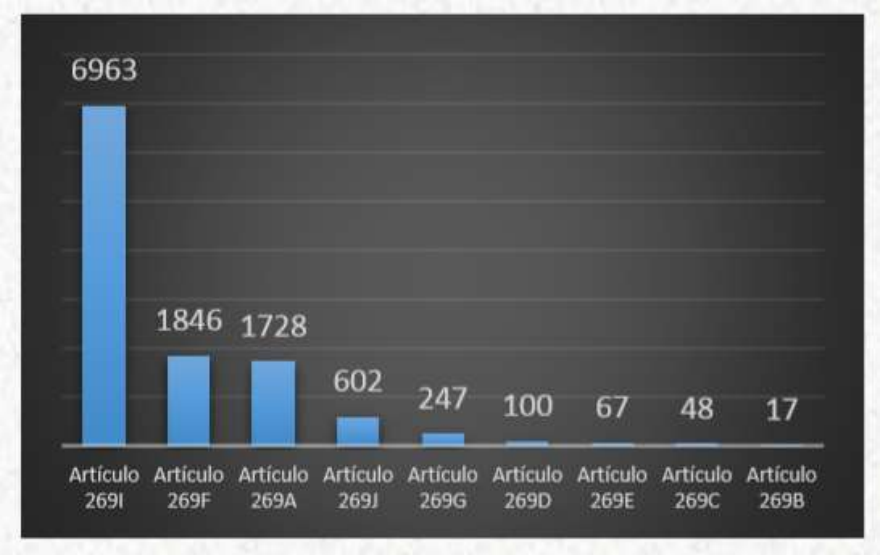
De acuerdo con el "Informe Cibercrimen 2017[60]" emitido por el CAI Virtual de la Policía Nacional en Colombia durante este periodo se recibieron 11.618 denuncias

---

[57] Declaraciones de Camilo Gutiérrez recuperadas de http://www.portafolio.co
[58] Kaspersky., op. cit, p. 1
[59] OEA. Comunicado de Prensa C-056/18 [en línea]. [Consultado 25 de septiembre de 2018]. Recuperado de: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-056/18
[60] COLOMBIA. POLICÍA NACIONAL. 2017. Informe Cibercrimen 2017. Recuperado de: https://caivirtual.policia.gov.co

por violación a la ley 1273 de 2009, dando un panorama de los delitos que más se denuncian en el país, tal como se aprecia en la Figura 9.

Figura 9. Delitos más denunciados en Colombia según ley 1273 de 2009



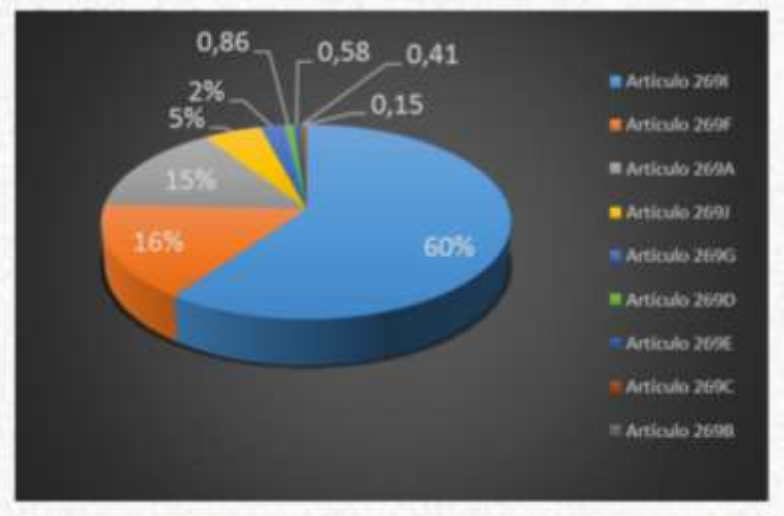
Fuente: https://caivirtual.policia.gov.co

En cuanto a las tipologías criminales denunciadas ante la Policía Nacional en el citado periodo de tiempo (Figura 10), el informe evidencia un aumento significativo en el número de estas por conductas delictivas que vulneraron la integridad personal, patrimonio económico de entidades público - privadas, así como la integridad, disponibilidad y confidencialidad de la información que circula a través del ciberespacio[61].

La tipología criminal con mayor frecuencia (60%) corresponde (por Ley 1273) al artículo 269I hurto por medios informáticos y semejantes; seguidos del artículo 269F, violación de datos personales con 16% y el artículo 269A, acceso abusivo a un sistema informático con el 15% de los reportes.

[61] Ibíd., p. 1

Figura 10. Tipologías criminales denunciadas ante la Policía Nacional



Fuente: https://caivirtual.policia.gov.co

6.1.2 Delitos Informáticos en Chile

El ciberataque perpetrado al Banco de Chile en mayo del 2018 terminó robando US$ 10 millones, el virus que afectó al sistema SWIFT de gestión de pagos de alto valor de transacciones entre bancos fue, de acuerdo con el análisis forense, un ataque internacional sofisticado y materializado por bandas de nivel mundial. Este hecho también afectó el normal funcionamiento de la entidad, ya que fue necesario bajar el servidor que guarda las claves de los clientes para evitar otras transacciones.

La Brigada de Cibercrimen de la Policía de Investigaciones de Chile se creó el año 2000 para hacer frente al sabotaje y espionaje informático, aunque este grupo ha crecido sus esfuerzos están orientados el tráfico de pornografía infantil, por lo que no es efectiva ni completa su estrategia.

De acuerdo con la publicación de Cristina Goyeneche[62] en Pressreader entre enero de 2017 y mayo de 2018, la Brigada de Cibercrimen solo recibió 13 denuncias por delitos informáticos cometidos contra empresas, pero el comisario de la brigada precisa que estos 13 casos no representan ni el 1% del total de ciberdelitos cometidos en el país.

Cristina Goyeneche[63] también precisa que las tres industrias más atacadas en el mundo, en este orden, son la banca, el retail y los servicios. Tres industrias muy intensivas en inversiones en tecnología, pero con poca preocupación por la ciberseguridad. Según The Boston Consulting Group, las empresas chilenas gastaron US$ 195,7 millones de dólares en ciberseguridad el 2017, equivalente al 0,07% del PIB, mientras que el promedio mundial es 0,12% del PIB.

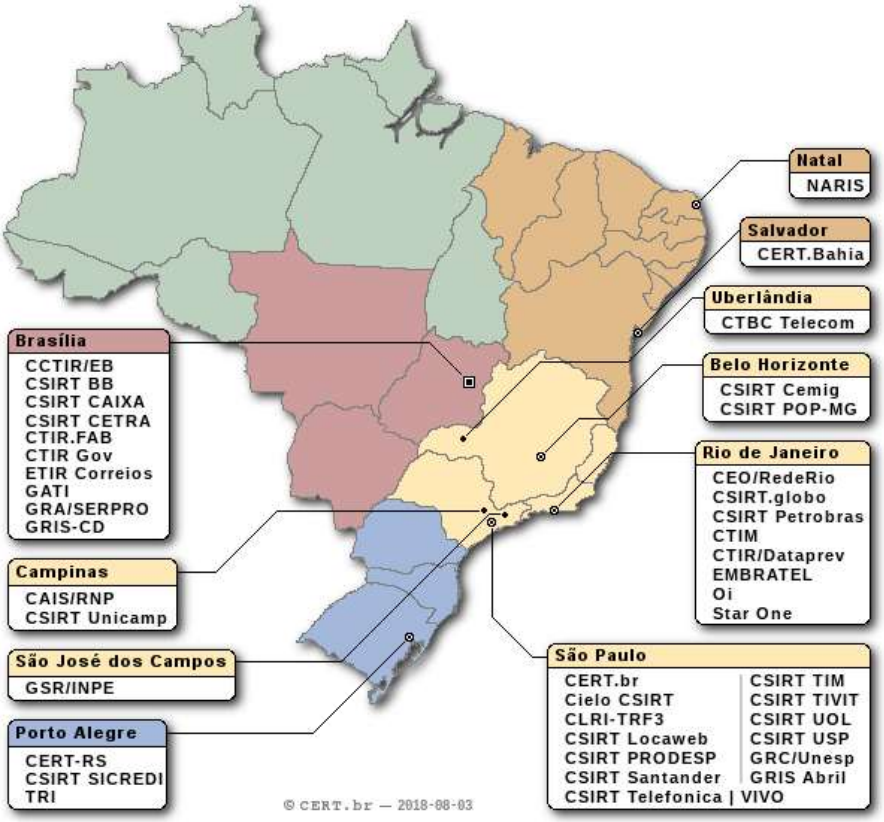
Tras el ataque al Banco de Chile se anunció la creación del Centro Nacional de Ciberseguridad Policial (Ciberpol), cuyo objetivo central es analizar las amenazas virtuales que afecten al país.

6.1.3 Delitos Informáticos en Brasil

Brasil cuenta con el Centro para Estudios, Respuesta y Tratamiento de Incidentes de Seguridad CERT.br liderado por el Centro de Información y Coordinación NIC.br y el Comité Directivo de Internet, y apoya a cualquier red brasileña conectada a Internet, los cuales lideran proyectos, llevan estadísticas y desarrollan capacitaciones permanentes sobre ciberseguridad, entre otras acciones.

[62] GOYENECHE MARIA CRISTINA. Ciberataques en Chile: en medio de la noche oscura. En: Pulso Pressreader. [en línea]. [Consultado 17 Junio de 2018]. Recuperado de: https://www.pressreader.com/
[63] Ibid., p. 1

Figura 11. Equipos Brasileños CSIRT

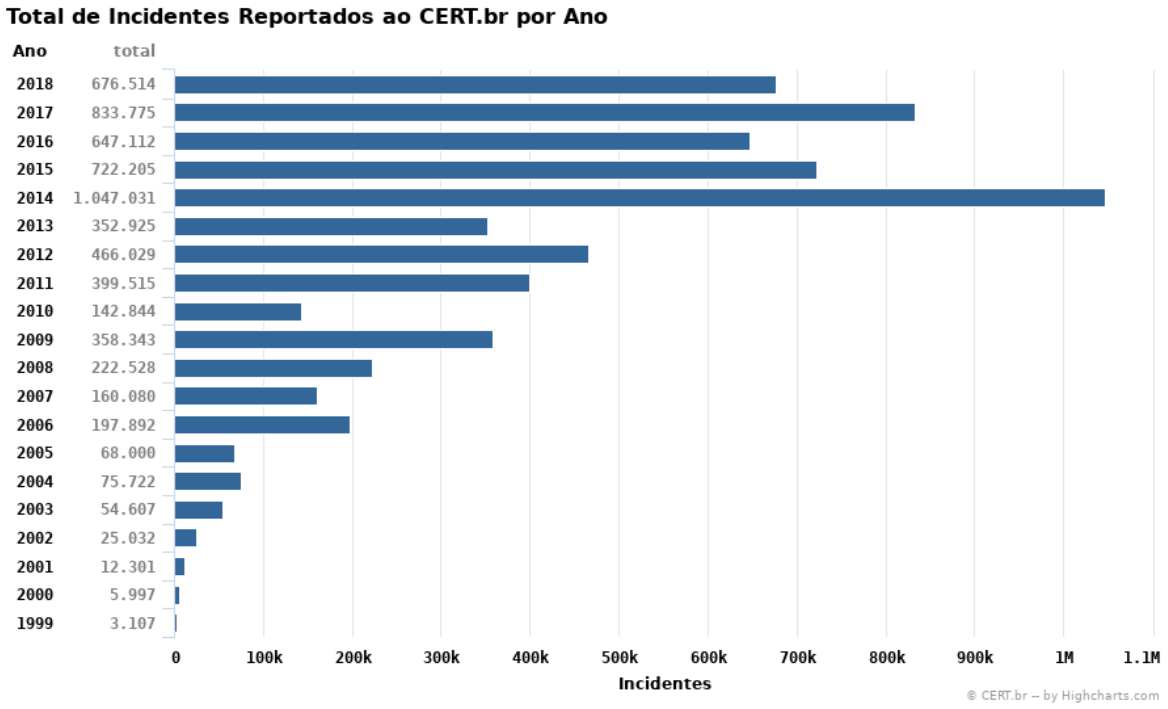


Fuente: https://www.cert.br/csirts/brasil/

Al revisar las estadísticas de los incidentes reportados al CIRT.br[64] desde 1999 hasta el 2018 se observa que la tendencia al alza con pequeñas fluctuaciones hasta el 2014 año con el mayor número de reportes (1.047.031); en 2015 y 2016 bajaron los reportes hasta 647.112, cifra que se disparó en el 2017 (833.775) y finalmente bajo a 676.514 incidentes reportados durante el 2018 como puede verse en la figura 12.

[64] BRASIL. CIRT.br. Centro para Estudios, Respuesta y Tratamiento de Incidentes de Seguridad de Brasil [en línea]. [Consultado 30 de agosto de 2019]. Recuperado de: https://www.cert.br

Figura 12. Incidentes por año en Brasil reportados a CSIRT



Fuente: https://www.cert.br/stast/incidentes/

Entre los hechos más relevantes del 2018 sobre los incidentes reportados al CIRT.br se encuentra que fueron recibidas 158,407 notificaciones sobre computadoras que participaron en ataques de denegación de servicio (DoS); los intentos de fraude totalizaron 37,684 reportes; el phishing clásico se redujo un 28% en comparación con el 2017; los ataques a servidores web totalizaron 41,193 notificaciones.

6.1.4 Delitos Informáticos en México

Revisar los delitos informáticos en México es hablar de una liga mayor en Latinoamérica y porque no, del mundo entero, y es que durante el 2018 este país centroamericano fue el tercero con más ciberataques (solo precedido por Estados

Unidos y el Reino Unido) según la aseguradora Lockton México[65] que precisa también en su informe la pérdida de 7.7 mil millones de dólares como consecuencia de los ciberataques.

El ataque al Banco Central de México en mayo del 2018 afectó a 5 compañías y el robo superó los 15 millones de dólares a través de falsas transferencias y de acuerdo a las investigaciones el procedimiento fue similar al ataque perpetrado al banco central de Banglades en 2016. Otro ataque importante en el que México resultó ser el país más afectado de Latinoamérica fuel el del virus WannaCry en 2017.

Para Lockton México los principales riesgos que existen hoy en día por un ciberataque son: Robo de datos de usuarios; Pérdida o eliminación de información; Robo de identidad; Fraude o extorsión; Secuestro de información; Robo de Propiedad Intelectual; Interrupción de servicios; Multas por organismos regulatorios; y Daño a la Reputación. Según precisa la aseguradora mexicana todas las actividades que deben realizarse posterior a un ataque cibernético "genera un costo muy alto que puede representar para algunas empresas la salida del mercado"[66]

6.1.5 Delitos Informáticos en El Salvador

De acuerdo con el artículo Cibercrimen e Informática Forense: Introducción y Análisis en el Salvador, de la Escuela Especializada en Ingeniería ITCA-FEPADE este Gobierno no ha establecido instituciones públicas dedicadas al manejo de la ciberseguridad y/o combate al Cibercrimen; de igual modo se debe trabajar

[65] Lockton México. El riesgo de ciberataques, una realidad palpable. [en línea]. [Consultado diciembre de 2018]. Recuperado de: http://www.lockton.com.mx/Website/media/10417/whitepaper-cyber-1.pdf
[66] Ibíd., p. 6

fuertemente en la cultura de ciberseguridad con campañas y estrategias educativas para toda la ciudadanía[67].

La Unión Internacional de Telecomunicaciones (ITU) en Ginebra, Suiza junto con ABI Research desarrollaron el Índice Mundial de Ciberseguridad (IMC) para 193 países Estados Miembros para medir su preparación ante el cibercrimen enfocados en cinco áreas de medición (Medidas jurídicas, Técnicas, Organizativas, Creación de Capacidades y Cooperación); de acuerdo con el informe del 2015[68] el Salvador se ubicó en el puesto 12 del ranking entre los países de América.

Tabla 6. Ranking 2015 para América del Índice Mundial de Ciberseguridad

Americas	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
United States of America*	1.0000	0.8333	0.8750	1.0000	0.5000	0.8235	1
Canada*	0.7500	1.0000	0.8750	0.8750	0.5000	0.7941	2
Brazil	0.7500	0.6667	0.8750	0.7500	0.5000	0.7059	3
Uruguay	1.0000	0.6667	0.6250	0.5000	0.5000	0.6176	4
Colombia	0.7500	0.5000	0.7500	0.7500	0.2500	0.5882	5
Argentina*	1.0000	0.3333	0.3750	0.5000	0.1250	0.4118	6
Chile*	0.7500	0.5000	0.2500	0.3750	0.2500	0.3824	7
Costa Rica*	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	8
Ecuador	0.2500	0.6667	0.1250	0.5000	0.2500	0.3529	8
Mexico*	0.2500	0.5000	0.1250	0.3750	0.3750	0.3235	9
Peru*	0.7500	0.3333	0.2500	0.1250	0.3750	0.3235	9
Panama	0.2500	0.5000	0.3750	0.2500	0.1250	0.2941	10
Jamaica*	0.7500	0.0000	0.1250	0.1250	0.3750	0.2353	11
El Salvador*	0.0000	0.3333	0.2500	0.1250	0.2500	0.2059	12
Guatemala	0.0000	0.3333	0.1250	0.3750	0.1250	0.2059	12
Paraguay*	0.0000	0.3333	0.1250	0.2500	0.2500	0.2059	12
Trinidad and Tobago	0.2500	0.0000	0.5000	0.1250	0.1250	0.2059	12
Venezuela	0.5000	0.3333	0.0000	0.2500	0.1250	0.2059	12
Barbados	0.5000	0.0000	0.1250	0.2500	0.1250	0.1765	13
Belize*	0.2500	0.0000	0.2500	0.1250	0.2500	0.1765	13
Bahamas*	0.7500	0.0000	0.0000	0.1250	0.1250	0.1471	14
Nicaragua*	0.5000	0.0000	0.2500	0.1250	0.0000	0.1471	14

Global Cybersecurity Index & Cyberwellness Profiles

Fuente: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

[67] ESCUELA ESPECIALIZADA EN INGENIERÍA ITCA-FEPADE. Cibercrimen e Informática Forense: Introducción y Análisis en el Salvador Revista Tecnológica N° 10. Enero - Diciembre 2017. p. 67

[68] ITU. Global Cybersecurity Index & Cyberwellness Profiles. [en línea]. [citado en 25 de abril de 2015]. Recuperado de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

Uno de los ciberataques más sonados en el Salvador es el llamado “Caso Troll Center” en el que fue clonado el sitio Web de un reconocido medio y difundieron una entrevista falsa con el presidente del Grupo LPG (La Prensa Gráfica) con el objetivo de desprestigiar el Periódico, por las deficientes herramientas legales y capacidades técnicas nadie fue condenado, pese a haber encontrado el sitio donde funcionaba el falso servidor y capturado en este a 5 personas implicadas.

6.2 Ciberseguridad en Latinoamérica

> La mayoría de los países de América Latina y el Caribe ya han establecido y puesto en funcionamiento los Equipos de Respuesta ante Emergencias Informáticas (CSIRT, por sus siglas en inglés) o capacidades y están ampliando los servicios prestados por estas unidades más allá de tener funciones reactivas, e incluyen servicios proactivos, preventivos, educativos y de gestión de la seguridad.[69]

La anterior afirmación es tomada del informe Ciberseguridad 2016 que la Organización de Estados Americanos – OEA y el Banco Interamericano de Desarrollo – BID donde también señalan que los países también deben invertir en investigación básica y aplicada de seguridad cibernética (innovación) y financiar generosamente las iniciativas de seguridad cibernética[70].

A continuación se revisa el panorama de los delitos y ataques informáticos más habituales en algunos países latinoamericanos, como Brasil, Chile, Colombia, México y El Salvador:

6.2.1 Ciberseguridad en Colombia

El 11 de septiembre de 2013, Colombia fue invitada por el Consejo de Europa a adherirse al Convenio de Budapest y lo materializo 5 años después mediante la

[69] BID. OEA. Informe Ciberseguridad 2016: ¿Estamos preparados en América Latina y el Caribe?. p. 33

[70] Ibíd., p. 33

aprobación del proyecto de ley 1928 del 2018, puede entenderse que los 48 artículos del convenio de Budapest están acogidos en Colombia en diferentes normas, como por ejemplo, la Ley 1273 de 2009 (de la protección de la información y de los datos.), la Ley 1581 de 2012 (protección de datos, divulgación y denuncia de las violaciones de seguridad), la Ley 527 de 1999 ("…acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales…") y otras normas, así como los Conpes 3701 de 2011 (lineamientos de política de ciberseguridad y ciberdefensa) y 3854 de 2016 (seguridad digital integral).

En Colombia los Lineamientos de Política para Ciberseguridad y Ciberdefensa del que trata el documento CONPES 3701[71] creó el equipo coordinador a nivel nacional en aspectos de seguridad informática ColCERT, para fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio; también se crea el Comando Conjunto Cibernético – CCOC, en cabeza de las fuerzas militares y el Centro Cibernético Policial – CCP liderado por la Policía Nacional, quienes operan con colaboración activa en la resolución de incidentes.

El Centro Cibernético Policial se encarga de activar su ruta de atención a través del CAI Virtual y su grupo de gestión de incidentes e investigación, es así como el CCP lleva a cabo la investigación y apoya la judicialización, entendiendo que es un delito informático tipificado por la ley 1273 de 2009 que se estudió en el capitulo anterior.

6.2.2 Ciberseguridad en Chile

[71] COLOMBIA. DNP. Conpes 3701 del 14 de julio de 2011, Lineamientos de Política para Ciberseguridad y Ciberdefensa

Las Fuerzas Armadas de Chile en sus múltiples divisiones comparten responsabilidades de defensa cibernética e información pero funcionalmente no logran ser una central de mando y control. Aunque el CSIRT-CL brinda respuesta a incidentes al gobierno desde el nivel nacional no está institucionalizado para abordar todo tipo de violaciones.

De acuerdo con el Informe de Ciberseguridad 2016[72], suplantación de identidad (phishing), malware y piratería informática son los tipos más frecuentes de ataques cibernéticos en el país.

> El Departamento de Investigación de Organizaciones Criminales (OS-9) y el Laboratorio de Criminalística de los Carabineros (LABOCAR), la policía nacional de Chile, llevan a cabo investigaciones y análisis forense digital respectivamente. Estas unidades han detenido con éxito numerosos criminales cibernéticos en los últimos años. Por último, los tribunales tienen una capacidad adecuada para manejar evidencia electrónica[73].

Este país ha adelantado algunas campañas para generar conciencia sobre la seguridad cibernética, pero aún no logra generar un impacto significativo para los grandes retos que ello denota; el sector privado esta mas sensibilizado en este aspecto.

6.2.3 Ciberseguridad en Brasil

> Brasil tiene varios de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), que van desde entidades administradas por el gobierno a equipos del sector privado o académicos. El Comité Gestor de Internet en Brasil (CGI.br) es el encargado de coordinar todas las iniciativas de servicios de Internet en el país y el Centro de Información de la Red Brasileña (NIC.br) trabaja para implementar este tipo de iniciativas. El equipo Nacional de Respuesta a Incidentes Informáticos de Brasil (CERT.BR), que opera bajo el CGI.br y el NIC.br, es responsable de la respuesta y coordinación a incidentes, capacitación y campañas de concientización. El Departamento de

[72] OEA. BID. op, cit. p. 62
[73] Ibíd, p. 62

> Seguridad de Información y Comunicaciones de Brasil también mantiene un CSIRT, el CTIR.gov, que proporciona servicios de respuesta a incidentes y recopilación de datos para la Administración Pública Federal[74].

El informe de Ciberseguridad 2016 de la OEA y el BID resalta las inversiones del gobierno de Brasil en TIC para promover el crecimiento económico y social y precisa que esta evolución lo ha convertido en un objetivo para los ataques y delitos cibernéticos que incluyen phishing, malware y ataques DDoS[75], entre otros.

Pese a los esfuerzos del gobierno a través de boletines y campañas de sensibilización la ciudadanía en un gran porcentaje no asimila los alcances de la problemática de la seguridad cibernética.

6.2.4 Ciberseguridad en México

El Equipo de Respuesta a Incidentes de Seguridad Informática de México, CERT-MX trabaja de forma colaborativa con otras entidades del gobierno y hace parte del FIRST (Forum for Incident Response and Security Teams). El CERT-MX monitorea la red pública de internet, las 24 horas al día los 365 días del año e intercambia información con agencias internacionales sobre las amenazas descubiertas.

> La División Científica de la Policía Federal de México investiga los delitos cibernéticos nacionales. Trabaja en estrecha colaboración con el CERT-MX y ha recibido capacitación por parte de organizaciones sin ánimo de lucro y de varias organizaciones internacionales. Informes recientes indican un aumento de la suplantación de identidad (phishing) y amenazas persistentes avanzadas en el país y una disminución de los ataques de denegación de servicio DoS (por sus siglas en inglés, Denial of Service)[76].

[74] OEA. BID. op, cit. p. 60
[75] Ibíd., p. 60
[76] Ibíd, p. 86

En materia de sensibilización sobre seguridad cibernética México ha dispuesto tanto en el gobierno como en el sector privado de muchas estrategias y programas de capacitación y orientación sobre esta área.

6.2.5 Ciberseguridad en El Salvador

El Ministerio de Justicia y Seguridad Pública de El Salvador es el principal organismo nacional encargado de la seguridad cibernética. Este país cuenta con un CSIRT nacional, el SalCERT, que responde a los ataques cibernéticos y coordina con otros equipos de respuesta regionales. El SalCERT ha tenido cierto éxito en el seguimiento y la lucha contra amenazas, pero su capacidad es limitada debido a restricciones presupuestales[77].

> La División de Ciberdelito de la Policía Nacional Civil investiga los delitos cibernéticos en el país y se ha asociado con la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD) para llevar a cabo ejercicios de construcción de capacidad. Dado que la División de Ciberdelito no tiene un laboratorio forense digital, recibe apoyo técnico del SalCERT y ha investigado con éxito varios casos, entre ellos uno en el que atrapó a un depredador sexual involucrado en captación infantil con fines sexuales (grooming)[78].

En cuanto a sensibilización de la ciudadanía Salvadoreña sobre ciberseguridad los esfuerzos del gobierno no son los mejores y esto se refleja en la poca conciencia de la sociedad frente a este tema; igual que en otros países latinoamericanos la empresa privada es quien mayor dinámica le imprime a las capacitaciones en seguridad cibernética.

[77] OEA. BID. op, cit. p. 72
[78] Ibíd., p. 72

7. IMPORTANCIA DE CONTROLAR TODA AMENAZA DETECTADA POR MUY BAJA QUE PAREZCA LA AFECTACIÓN.

Se ha planteado hasta el momento una serie de conceptos referentes a la seguridad de la información y la seguridad informática, se inicia con la definición de riesgo que brinda el diccionario de la RAE y las nociones de amenaza, vulnerabilidad y el riesgo informático como tal; se revisa las guías de análisis de riesgo de Magerit V3 y la ISO 27002 para el despliegue de los controles que se deben aplicar a toda posible vulneración del sistema.

Para evitar cualquiera de los ataques que pueda sufrir el sistema, como los descritos en el apartado anterior, es necesario disponer de recursos económicos, humanos y técnicos que permitan de cierto modo, proteger los activos informáticos, pero es aquí, en este punto del escrito, en el que se requiere tener la mayor atención del lector, puesto que, algunas compañías pese a tener todos los recursos mencionados y las herramientas necesarias para lograr un gran fortín de su sistema, terminan siendo atacados de la manera menos esperada a través de un equipo, servicio, lugar o empleado (considerado activo de bajo valor según su análisis) que no les generó la menor preocupación al equipo de seguridad informática, ni a los altos mandos de la organización.

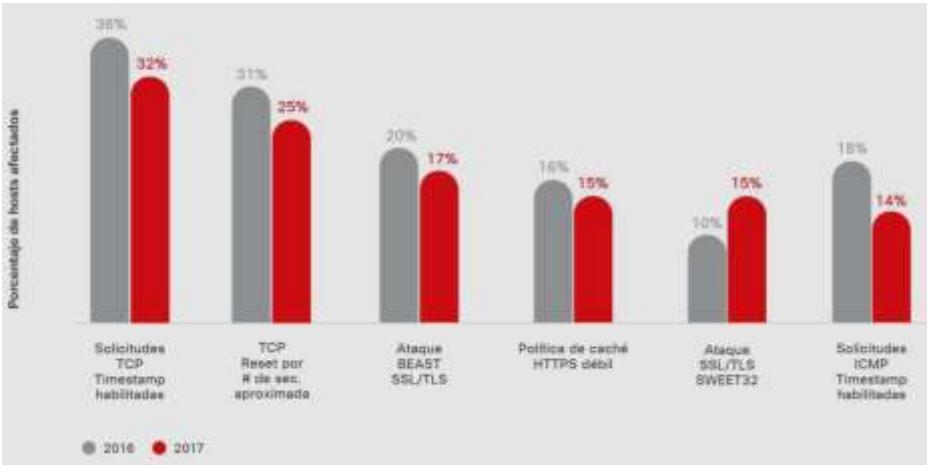
De acuerdo con los expertos en seguridad de SAIN Corporation[79] compañía de soluciones de seguridad y socio de Cisco “las vulnerabilidades de baja gravedad a menudo no se remedian durante años porque las empresas o no saben que existen o no las consideran riesgos importantes”. Sin embargo, estas brechas de seguridad pequeñas, pero significativas, podrían proporcionar a los adversarios caminos hacia los sistemas.

SAINT examinó los datos de exposición a la vulnerabilidad compilados de más de

[79] SAIN CORPORATION. Reporte Anual de Ciberseguridad Cisco 2018. EE.UU, 2018. p. 46

10,000 hosts en 2016 y 2017[80] y elaboró una lista de las principales vulnerabilidades detectadas con mayor frecuencia en las organizaciones bajo estudio, lo que indica que las vulnerabilidades de baja gravedad ocurren con mayor frecuencia tal como se muestra en la figura 13., a continuación:

Figura 13. Vulnerabilidades de baja gravedad más detectadas, 2016-2017



Fuente: SAIN Corporation

De acuerdo con la grafica anterior se puede evidenciar que las vulnerabilidades más comunes son de baja gravedad, pero de alto riesgo, por ejemplo las Solicitudes TCP Timestamp habilitadas ocupan el primer lugar con el 36% en 2016 y el 32% en 2017, esta vulnerabilidad brinda información sobre cuánto tiempo ha estado en funcionamiento un equipo o cuándo se reinició por última vez, esto en el buen olfato de un atacante le permite identificar debilidades en parches y podría explotar la máquina.

Esto permite incorporar al análisis planteado en este capítulo que no solo se trata de presupuesto y de altas inversiones (culpando solo a la alta dirección) para atender y controlar los riesgos, puesto que esta y muchas vulnerabilidades de este

[80] Ibíd., p. 46

tipo se corrigen fácilmente con un par de comandos o actualizando un parche, pero como durante el análisis de riesgo situaciones de este tipo fueron detectadas, pero su valoración o nivel de riesgo fue menor en comparación con otras amenazas, se le resta importancia y queda allí identificado en el análisis pero sin ninguna protección, tal vez este tipo de situaciones son la bases para que el experto Argentino Fabián Chiera, jefe de seguridad digital de la compañía Eleven Path, filial de Telefónica, manifestase en una entrevista con la agencia EFE, en el Salvador que “la aplicación de medidas enfocadas a la seguridad cibernética ha quedado en rezago en algunos países de Latinoamérica[81]” y que es necesario "quitarnos de la cabeza que implementar medidas de ciberseguridad es costoso y complicado"[82], en el ámbito laboral agregó que “una pequeña empresa que no tenga recursos económicos suficientes para invertir en programas de seguridad informática costosos puede hacer uso de muchas alternativas para proteger los datos e información que llevan” y que aplicar la ciberseguridad requiere de "estrategias bien elaboradas que estén a cargo de organismos y personas adecuadas para implementar planes de protección"[83].

Pero según la referencia de ISO/IEC27001 **a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados[84].** Y esto es un mensaje claro para los responsables de la gestión del riesgo, por lo que aquí se pregunta ¿qué razón de peso se tiene para decidir no establecer un control a una vulnerabilidad detectada? ¿Será que existen razones de peso para no establecer un control?

[81] AGENCIA EFE. Experto argentino señala "rezago" en seguridad cibernética en Latinoamérica [en línea]. [citado en 13 de julio de 2018]. Recuperado de: https://www.efe.com/efe/america/tecnologia/experto-argentino-senala-rezago-en-seguridad-cibernetica-latinoamerica/20000036-3688924#
[82] Ibíd., p 1
[83] Ibíd., p 1
[84] ISO 27001 EN ESPAÑOL. [En línea]. [Consultado 5 de julio de 2019]. Recuperado de: http://www.iso27000.es/iso27000.html

Ante las cuestiones anteriores se sugiere por parte del autor no responder automáticamente con una serie de excusas (algunas muy valederas) y por el contrario revisen con calma el costo de los ataques que pueden sufrir en caso de no implementar un control, es así como en el Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018 inmerso en el Reporte Anual Cisco 2018[85] precisa que "El miedo a las violaciones se basa en el costo financiero de los ataques, que ya no es un número hipotético. Las infracciones causan un daño económico real a las organizaciones, daños que pueden tardar meses o años en resolverse. Según los encuestados del estudio, más de la mitad (53 por ciento) de todos los ataques resultaron en daños financieros de más de USD $500,000, que incluyen, entre otros, pérdida de ingresos, clientes, oportunidades y costos de bolsillo", tal como muestra la Figura 14.

Figura 14. 53% de los ataques resultan en daños de $500.000 o más

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

El Reporte Anual Cisco 2018[86] también señala que los profesionales de la

[85] CISCO SYSTEM. Reporte Anual de Ciberseguridad Cisco 2018. EE.UU, 2018. p. 49
[86] Ibíd., p. 49

seguridad de las organizaciones encuestadas citan el presupuesto, la interoperabilidad y el personal como sus principales limitaciones a la hora de administrar la seguridad.

Figura 15. Mayor obstáculo para las restricciones presupuestarias de seguridad

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

CONCLUSIONES

La metodología Magerit en su versión 3.0 permite de una manera sencilla realizar un análisis de riesgos para la identificar amenazas y valorar los riesgos informáticos y para ello cuenta con tres libros que orientan sobre cada uno de los pasos, pero al igual que otras metodologías son los dueños y empleados de la organización los que deciden cuan preciado son los activos.

Se debe ser “ambicioso” durante el análisis de riesgos informáticos en la valoración de los riesgos, ya que a partir de sus resultados se implementaran las medidas de protección sobre los activos de información; no hacerlo puede costar el desplome de todas medidas adoptadas y hasta poner en riesgo la continuidad del negocio.

La ISO (The International Organization for Standardization) y la IEC (International Electrotechnical Commission) originaron la serie 27000 que corresponde a las normas que respaldan la seguridad de la información, siendo la ISO/IEC 27002 aquella que establece el código de mejores prácticas para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones, mediante una guía que describe cómo se pueden establecer los controles. Pero estos controles deben ser aplicados con base en una evaluación de riesgos como se explicó con la guía de Magerit 3.0., dando la mayor importancia a cada activo y controlando todo lo que genere riesgo.

Las cifras sobre ataques informáticos en Latinoamérica van en aumento y los ciberdelincuentes no escatiman esfuerzos ni se limitan a las viejas técnicas, por el contrario día a día van sofisticando sus estrategias y herramientas de ataque, de hecho la ingeniería social y el estudio de sus víctimas es una tarea que realizan con mucha pasión, ya que los beneficios económicos obtenidos por medio de

estas prácticas se han vuelto realmente atractivas y esto ha cambiado la ideología de muchos atacantes.

La gestión de incidentes realmente efectiva debe orientarse a que durante el análisis el apetito de riesgos sea mayor, teniendo en cuenta también a los activos de valoración media y baja.

Ante los altos directivos, el equipo de gestión de riesgos debe estar claro al momento de exigir el presupuesto y advertir con estadísticas recientes que cada riesgo o amenaza detectada por muy bajo que parezca su impacto puede incluso ser el detonador de una hecatombe para todo el sistema, es decir, que puede en algún momento tirar por la borda toda la inversión puesta en los otros controles, por ejemplo comprar un candado enorme y costoso para la puerta e invertir en un avanzado equipo de monitoreo con cámaras infrarrojas, pero no determinar un control para que la llave del candado no caiga en manos equivocadas o no incluir en el presupuesto alguien que vigile las cámaras.

Finalmente todo el personal, en especial aquellos ingenieros y técnicos cuya función principal es evitar que la organización sea víctima de un ataque informático, deben realizar todas las actividades de control y vigilancia establecidas en las políticas de seguridad día tras días (no cuando se los recuerde una auditoría) porque no solo se trata de presupuesto y de altas inversiones (culpando solo a la alta dirección) para atender y controlar los riesgos, ya que muchas vulnerabilidades se pueden corregir con algunos comandos o actualizando un parche, bloqueando un servicio, etc., todo esto sin lugar a dudas invita al lector a valorar la importancia de controlar todas las amenazas detectadas.

RECOMENDACIONES

A lo largo de este trabajo se revisaron conceptos y se analizaron dos herramientas importantes dentro de un sistema de gestión de seguridad informática como son la guía Magerit 3.0 y la guía de buenas prácticas ISO/IEC 27002 y para justificar las exigencias sobre un mayor apetito de riesgos para aplicar los controles hemos presentado cifras actuales y contundentes sobre el aumento de los ataques informáticos en Latinoamérica, lo que debiera ser suficiente para reflexionar y tener en cuenta lo aquí expuesto, sin embargo, como única recomendación se plantea aprovechar al máximo los controles de la ISO 27002 y no limitarse a estos, ya que cada organización de acuerdo a su visión y los resultados del análisis de riesgo puede implementar otras medidas o mecanismos que le permita blindar todo su sistema.

BIBLIOGRAFÍA

ANDER-EGG, Ezequiel. Cómo elaborar monografías, artículos científicos y otros textos expositivos, Homo Sapiens Ediciones. Madrid. 2017.

AGENCIA EFE. Experto argentino señala "rezago" en seguridad cibernética en Latinoamérica [En línea]. [Consultado 13 de julio de 2018]. Disponible en: https://www.efe.com/efe/america/tecnologia/experto-argentino-senala-rezago-en-seguridad-cibernetica-latinoamerica/20000036-3688924#

BID. OEA. Informe Ciberseguridad 2016: ¿Estamos preparados en América Latina y el Caribe? [En línea]. [Consultado 12 de junio de 2019]. Disponible en: http://www.observatoriociberseguridad.com

BRASIL. CIRT.BR. Centro para Estudios, Respuesta y Tratamiento de Incidentes de Seguridad de Brasil: Incidentes reportados a CERT.br - enero a diciembre de 2018 [En línea]. [Consultado 30 de agosto de 2019]. Disponible en: https://www.cert.br/stats/incidentes/2018-jan-dec/analise.html

CANO, Jeimy. Modelo PERIL, Repensando el gobierno de la seguridad de la información desde la inevitabilidad de la falla. En: VII Congreso Iberoamericano de Seguridad Informática. Sangolqui (Quito). Universidad de las Fuerzas Armadas del Ecuador - ESPE. 2015. p 13.

CERVERA OLIVARES, David, et al. Complementos de formación disciplinar. Tecnología. 2010.

COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Documento Conpes 3701, Lineamientos de Política para Ciberseguridad y Ciberdefensa, Bogotá D.C., 14 de julio de 2011

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. [Consultado 19 de junio de 2018]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. POLICÍA NACIONAL. 2017. Informe Cibercrimen 2017. [En línea]. [Consultado 19 de junio de 2018]. Disponible en: https://caivirtual.policia.gov.co

COSTAS, Jesús. Seguridad informática, RA-MA Editorial, 2014.

CNN ESPAÑOL. Cada 33 segundos hay un ataque cibernético en América Latina. [En línea]. [Consultado 10 de junio de 2018]. Disponible en: https://cnnespanol.cnn.com/2017/09/19/cada-33-segundos-hay-un-ataque-cibernetico-en-america-latina/

DALTABUIT, E. La seguridad de la información. Balderas, México. Limusa. 2007.

ESCUELA ESPECIALIZADA EN INGENIERÍA ITCA-FEPADE. Cibercrimen e Informática Forense: Introducción y Análisis en el Salvador. En: Revista Tecnológica N° 10. Enero - Diciembre 2017. p 67

ESET. ESET Security Report Latinoamérica 2017. Incidentes de seguridad en empresas latinoamericanas. Argentina. Ed. Laboratorio de Investigación de ESET. 2017.

ESPAÑA. CENTRO SUPERIOR DE INFORMACIÓN DE LA DEFENSA, “Glosario de Términos de Criptología”, 3ª edición, 1997. En: Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 99

ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: Libro I – Método. Madrid. 2012. 127p.

_____ MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: Libro II – Catálogo de Elementos. Madrid. 2012. 75p.

_____ MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: Libro III – Guía de Técnicas. Madrid. 2012. 42p.

FERRERO, Eduardo. Análisis y gestión de riesgos en iMat del sistema de información de I.C.A.I. Tesis Universidad Pontificia Comillas Escuela Técnica Superior de Ingeniería (ICAI), Madrid, Junio del 2006, p. 140.

GASCÓ Ema, et al. Conceptos sobre seguridad informática, Madrid. MacMillan Profesional. 2013.

GÓMEZ, Álvaro. Seguridad en equipos informáticos, RA-MA Editorial, 2014.

GÓMEZ, L. y ÁLVAREZ, A. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, AENOR - Asociación Española de Normalización y Certificación, 2012.

GÓMEZ, J. Seguridad en sistemas operativos Windows y GNU/Linux. Bogotá. Firewall de Windows. Bogotá. 2012.

GUILLENSON, M. Administración de Bases de Datos. Seguridad de los Datos. México. Limusa Wiley. 2006. p 271

INTERNATIONAL TELECOMMUNICATION UNION ITU. Global Cybersecurity Index & Cyberwellness Profiles. [en línea]. [Consultado 25 de abril de 2015]. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

ISO 17799. Código de práctica para la gestión de la seguridad de la información. 2005.

ISO27001.ES. El portal de ISO 27001 en Español. Serie 27K. 2017. [En línea]. [Consultado 5 de julio de 2019]. Disponible en: http://www.iso27000.es/iso27000.html

KASPERSKYLAB. Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina. Argentina. 2017. [En línea]. [Consultado 8 de junio de 2018]. Disponible en: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

LOCKTON MÉXICO. El riesgo de ciberataques, una realidad palpable. [En línea]. [Consultado 20 de diciembre de 2018]. Disponible en: http://www.lockton.com.mx/Website/media/10417/whitepaper-cyber-1.pdf

PONFERRADA, Javier. Tipos de ataques y atacantes en Ciberseguridad. En: Ticarte.com [en línea]. [Consultado 12 de junio de 2019]. Disponible en: http://www.ticarte.com/contenido/tipos-de-ataques-y-atacantes-en-ciberseguridad.

PORTAFOLIO.CO. El 46% de las empresas colombianas sufrieron un ataque informático. 2017. [En línea]. [Consultado 8 de junio de 2018]. Disponible en: http://www.portafolio.co/negocios/empresas/el-46-de-las-empresas-colombianas-sufrieron-un-ataque-informatico-507228

RAMOS, L. A. Seguridad Informática. España, 2014. p. 54

REAL ACADEMIA ESPAÑOLA, *Diccionario de la Lengua Española* 23ª ed. Definición de Riesgo. [En línea]. [Consultado 10 de junio de 2019]. Disponible en: https://dle.rae.es/?id=WT8tAMI

UNIVERSIDAD DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme? 2016. Valencia, España. [En línea]. [Consultado 8 de junio de 2018]. Disponible en: https://www.universidadviu.es.

ZURICH INSURANCE GROUP. Beyond Data Breaches: Global Interconnections of Cyber Risk: Risk Nexus. Atlantic Council. Switzerland. Ed. The Atlantic Council. 2016. p. 6

ZURICH INSURANCE GROUP. Beyond Data Breaches: Global Interconnections of Cyber Risk: Risk Nexus. Atlantic Council, 2014. p.

RODRÍGUEZ, José y PERALTA, Ignacio. Gestión de Riesgos Magerit. España, TiThink, 2013

ANEXOS

ANEXO A

(Controles y objetivos de Dominios A5 y A6)

A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**	
A5.1	Orientación de la dirección para la gestión de la seguridad de la información	
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes		
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**	
A6.1	Organización interna	
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad

A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A6.2	Dispositivos móviles y teletrabajo	
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles		
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO B

(Controles y objetivos del Dominio A7)

A7	SEGURIDAD DE LOS RECURSOS HUMANOS	
A7.1	Antes de asumir el empleo	
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A7.2	Durante la ejecución del empleo	
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A7.3	Terminación y cambio de empleo	
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o		

terminación de empleo		
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO C

(Controles y objetivos del Dominio A8)

A8	GESTION DE ACTIVOS	
A8.1	Responsabilidad por los activos	
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.		
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A8.2	Clasificación de la información	
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A8.3	Manejo de medios	
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios		

A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO D

(Controles y objetivos de Dominios A9 y A10)

A9	CONTROL DE ACCESO	
A9.1	Requisitos del negocio para el control de acceso	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A9.2	Gestión de acceso de usuarios	
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A9.2.6	Retiro o ajuste de	Control: Los derechos de acceso de todos los empleados y de

	los derechos de acceso	usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A9.3	Responsabilidades de los usuarios	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A9.4	Control de acceso a sistemas y aplicaciones	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.
A10	**CRIPTOGRAFIA**	
A10.1	Controles criptográficos	
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información		
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas,

		durante todo su ciclo de vida.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO E

(Controles y objetivos del Dominio A11)

A11	SEGURIDAD FISICA Y DEL ENTORNO	
A11.1	Áreas seguras	
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A11.2	Equipos	
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de

		suministro.
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO F

(Controles y objetivos del Dominio A12)

A12	SEGURIDAD DE LAS OPERACIONES	
A12.1	Procedimientos operacionales y responsabilidades	
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A12.2	Protección contra códigos maliciosos	
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A12.3	Copias de respaldo	
Objetivo: Proteger contra la perdida de datos		
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

A12.4	Registro y seguimiento	
Objetivo: Registrar eventos y generar evidencia		
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A12.5	Control de software operacional	
Objetivo: Asegurarse de la integridad de los sistemas operacionales		
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A12.6	Gestión de la vulnerabilidad técnica	
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas		
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A12.7	Consideraciones sobre auditorias de sistemas de información	
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos		
A12.7.1	Gestión de las vulnerabilidades	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que

	técnicas	se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO G

(Controles y objetivos del Dominio A13)

A13	SEGURIDAD DE LAS COMUNICACIONES	
A13.1	Gestión de la seguridad de las redes	
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A13.1.2	"Seguridad de los servicios de red"	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A13.2	Transferencia de información	
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A13.2.1	Políticas y procedimientos de información	"Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones."
A13.2.2	"Acuerdos sobre transferencia de información"	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO H

(Controles y objetivos del Dominio A14)

A14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
A14.1	Requisitos de seguridad de los sistemas de información	
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A14.2	Seguridad en los procesos de Desarrollo y de Soporte	
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a

	después de cambios en la plataforma de operación	prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A14.3	Datos de prueba	
Objetivo: Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de datos de prueba	

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO I

(Controles y objetivos del Dominio A15)

A15	RELACIONES CON LOS PROVEEDORES	
A15.1	Seguridad de la información en las relaciones con los proveedores.	
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A15.1.1	Política de segurida de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A15.1.3	Cadena de suministro de TIC	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A15.2	Gestión de la prestación de servicios de proveedores	
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores		
A15.2.1	Seg/to y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO J

(Controles y objetivos del Dominio A16)

A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	
A16.1	Gestión de incidentes y mejoras en la seguridad de la información	
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.

	información	
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO K

(Controles y objetivos del Dominio A17)

A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	
A17.1	Continuidad de Seguridad de la información	
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A17.2	Redundancias	
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO L

(Controles y objetivos del Dominio A18)

A18	CUMPLIMIENTO	
A18.1	Cumplimiento de requisitos legales y contractuales	
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A18.2	Revisiones de seguridad de la información	
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		
A18.2.1	Revisión independiente de la	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los

	seguridad de la información	objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: Anexo A ISO/IEC 27001:2013

ANEXO M

(Resumen Analítico Especializado - RAE)

TEMA	ANALISIS Y GESTION DEL RIESGO INFORMATICO
TÍTULO	IMPORTANCIA DE CONTROLAR TODAS LAS AMENAZAS DETECTADAS A TRAVÉS DE MAGERIT V.3 E ISO/ IEC 27002 SEGÚN ANÁLISIS DE ATAQUES INFORMÁTICOS EN LATINOAMÉRICA
AUTOR	Rodríguez Arroyo, Hugo Alfonso
FUENTES BIBLIOGRÁFICAS	37 Fuentes Bibliográficas se presentan, entre estas se encuentran, Textos Impresos y Digitales, Información estadística, Artículos Web de destacadas empresas de seguridad informática como Kaspersky y Normas Técnicas (ISO y Magerit).
AÑO	2019
RESUMEN	Monografía como opción de grado para optar al título de especialización en seguridad informática. Es una investigación sobre los ataques informáticos en Latinoamérica que tiene como objetivo principal revisar la importancia de los resultados de un análisis de riesgos informáticos para que los profesionales de la seguridad informática se concienticen que toda amenaza detectada debe ser controlada mediante el estudio de la metodología MAGERIT V.3 y la norma ISO/IEC 27002:2013.
PALABRAS CLAVES	Sistema de Gestión de Seguridad, Magerit, ISO/IEC 27002, Análisis de Riesgo, Gestión del Riesgo, Seguridad Informática, Ataque Informático, Amenazas, Riesgo Informático, Latinoamérica.
CONTENIDOS	El documento inicia con una introducción acerca de la forma

	en que las compañías establecen su sistema de gestión de seguridad de la información – SGSI y la implementación de los controles que consideran necesarios para afrontar los riesgos informáticos identificados; luego nos indica que existen diferentes metodologías para la gestión del riesgo informático, pero toma como base del estudio la Guía Magerit 3.0 elaborada por el Consejo Superior de Administración Electrónica de España, la cual inicia con la identificación de los activos de información, incluyendo datos, hardware, recurso humano y software a los que otorga un valor y luego identifica las amenazas, riesgos y vulnerabilidades de cada uno de estos activos hasta determinar cuáles son los riesgos encontrados y clasificados por la complejidad y afectación que puede ocasionar y de este modo definir los controles para estos. Pese a que Magerit incorpora los controles para cada riesgo el autor separa esta parte del ejercicio y opta por implementar los controles con base a la norma ISO/IEC 27002 de 2013 que goza del respaldo y trascendencia de la Organización Internacional de Normalización. En otro apartado importante el escrito revisa algunos datos estadísticos plasmados en diferentes informes y artículos sobre incidentes informáticos en Latinoamérica y las terribles consecuencias que estos ataques tienen sobre las organizaciones victimas y que van desde una simple interrupción de servicios hasta la perdida y secuestro de información que en muchos casos obligan al cierre del negocio o dejan pérdidas económicas que son realmente significativas; frente a este panorama presenta un enfoque

	muy interesante, ya que destaca como muchas organizaciones víctimas de ataques asignaron recursos para proteger sus activos informáticos, pero que no fueron los que esperaban los encargados de la seguridad informática o al momento de definir los controles sobre los riesgos solo se limitaron a aquellos que obtuvieron una valoración alta o critica, dejando de lado las pequeñas vulnerabilidades que, en su afán de bajar los costos, no creyeron oportunas para tenerlas en cuenta, sin embargo la evolución de los ciberataques y las técnicas empleadas han permitido que el delincuente informático sea estudioso, creativo y eficiente para aprovechar el minino descuido de su víctima. El autor finaliza resaltando el valor de los resultados obtenidos de un análisis de riesgos informáticos para que los profesionales de la seguridad informática se concienticen que toda amenaza detectada debe ser controlada sin importar su baja valoración, puesto que al fin y al cabo los ciberdelincuentes podrán aprovecharse de estas.
DESCRIPCION DEL PROBLEMA	Muchas empresas destinan un porcentaje de su presupuesto para proteger sus activos informáticos, de este rubro normalmente se realiza un análisis de riesgos informáticos que muestra el panorama real de la empresa en términos de amenazas, vulnerabilidades y el impacto que tendría en caso de materializarse alguna de las amenazas, pero al momento de gestionar el riesgo informático detectado durante el análisis solo se enfocan en aquellos cuya valoración es alta, dejando de lado las pequeñas debilidades que para los ciberdelincuentes son suficientes

	para vulnerar un sistema cualquiera.
OBJETIVOS	Analizar la metodología MAGERIT V.3 y la norma ISO/IEC 27002:2013. Interpretar estadísticas sobre ataques de seguridad informática en Latinoamérica. Revisar la importancia de controlar toda amenaza detectada por muy baja que parezca la afectación.
METODOLOGÍA	La metodología utilizada es la Investigación Acción Participativa, en la que el autor parte de la revisión de datos estadísticos de fuentes secundarias para generar conciencia y buscar una actitud de cambio de los encargados de la seguridad informática y los altos mandos de las organizaciones para que todas las amenazas y riesgos detectados por un análisis de riesgo le sean aplicados los controles necesarios, sin excluir o descuidar aquellos con baja valoración, como normalmente viene ocurriendo.
PRINCIPALES REFERENTES TEÓRICOS	GASCÓ Ema, et al. Conceptos sobre seguridad informática, Madrid. MacMillan Profesional. 2013. RAMOS, L. A. Seguridad Informática. España, 2014. p. 54 ISO 17799. Código de práctica para la gestión de la seguridad de la información. 2005.
PRINCIPALES REFERENTES CONCEPTUALES	GÓMEZ, L. y ÁLVAREZ, A. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, AENOR - Asociación Española de Normalización y Certificación, 2012. Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid, 2012. p. 99

CONCLUSIONES	El autor concluye que la metodología Magerit en su versión 3.0 permite de una manera sencilla realizar un análisis de riesgos para identificar amenazas y valorar los riesgos informáticos y para ello cuenta con tres libros que orientan sobre cada uno de los pasos, pero al igual que otras metodologías son los dueños y empleados de la organización los que deciden cuan preciado son los activos. Se debe ser “ambicioso” durante el análisis de riesgos informáticos, en lo que respecta a la valoración de los riesgos, ya que a partir de sus resultados se implementaran las medidas de protección sobre los activos de información; no hacerlo puede costar el desplome de todas medidas adoptadas y hasta poner en riesgo la continuidad del negocio. La ISO (The International Organization for Standardization) y la IEC (International Electrotechnical Commission) originaron la serie 27000 que corresponde a las normas que respaldan la seguridad de la información, siendo la ISO/IEC 27002 aquella que establece el código de mejores prácticas para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones, mediante una guía que describe cómo se pueden establecer los controles. Pero estos controles deben ser aplicados con base en una evaluación de riesgos como lo explicamos con la guía de Magerit 3.0. dando la mayor importancia a cada activo y controlando todo lo que genere riesgo. Las cifras sobre ataques informáticos en Latinoamérica van

	en aumento y los ciberdelincuentes no escatiman esfuerzos ni se limitan a las viejas técnicas, por el contrario día a día van sofisticando sus estrategias y herramientas de ataque, de hecho la ingeniería social y el estudio de sus víctimas es una tarea que realizan con mucha pasión, ya que los beneficios económicos obtenidos por medio de estas prácticas se han vuelto realmente atractivas y esto ha cambiado la ideología de muchos atacantes. La gestión de incidentes realmente efectiva debe orientarse a que durante el análisis el apetito de riesgos sea mayor, teniendo en cuenta también a los activos de valoración media y baja. Ante los altos directivos el equipo de gestión de riesgos debe ser claro al momento de exigir el presupuesto y advertir con estadísticas recientes que cada riesgo o amenaza detectada por muy bajo que parezca su impacto puede incluso ser el detonador de una hecatombe para todo el sistema. Todo el personal debe realizar las actividades de control y vigilancia establecidas en las políticas de seguridad todos los días (no cuando se los recuerde una auditoría) porque no solo se trata de presupuesto y de altas inversiones (culpando solo a la alta dirección) para atender y controlar los riesgos, ya que muchas vulnerabilidades se pueden corregir con algunos comandos o actualizando un parche, bloqueando un servicio, etc.

Fuente: El Autor