IMPACTO DE LAS VULNERABILIDADES CIBERNÉTICAS EN LA EVALUACIÓN DE LA GESTIÓN DEL RIESGO PARA LAS PYMES

JAVIER ALEXANDER ANAYA MORENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
2021

Impacto de las vulnerabilidades cibernéticas en la evaluación de la gestión del riesgo para las pymes

JAVIER ALEXANDER ANAYA MORENO

DIRECTORA:

ING. YENNY STELLA NÚÑEZ ÁLVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

DEDICATORIA

Dedico este trabajo a mis hijos Santiago Anaya Castiblanco y Emmanuel Anaya Pérez que son la fuente de mi fortaleza, son los que me inspiran a ser mejor cada día como persona y como profesional, para lograr ser un ejemplo con el pasar de los años. No puedo olvidar tampoco a cada uno de mis familiares que estuvieron a mi lado luchando hombro a hombro que me vieron caer pero estuvieron hay para levantarme y ser ese apoyo incondicional.

AGRADECIMIENTOS

Primero que todo agradezco a mi señora madre por estar siempre a mi lado por ser mi apoyo, por ser la mujer luchadora la cual no dejaba ver que estaba derrotada en ninguna adversidad, por enseñarme a luchar cada día por los sueños y poder alcanzarlos. También agradezco a mi difunto hermano que desde el cielo está acompañándonos en cada una de nuestras aventuras, por enseñarme en vida a lograr cada una de las metas que uno se planeaba.

A la Universidad Nacional Abierta y A Distancia – UNAD – por abrir las puertas de la nueva enseñanza, a cada uno de los tutores que a lo largo de los años nos enseñan a vivir la vida laboral de la mejor manera.

A la Dra. Constanza Abadía la cual fue la persona que desde la conocí estuvo siempre a mi lado no solo por terminar mi carrera sino por ser cada día mejor persona y para finalizar dar gracias a Dios porque sin el nada sería posible en poner cada persona en el lugar correcto para poder levantarme de mis fracasos.

TABLA DE CONTENIDO

INTRODUCCIÓN 13
1. PLANTEAMIENTO DEL PROBLEMA 15
2. JUSTIFICACIÓN 17
3. OBJETIVOS 19
3.1 Objetivo General 19
3.2 Objetivos Específicos 19
4. MARCO CONCEPTUAL Y TEÓRICO 20
4.1 Principios de la seguridad de la información 22
4.1.1 Confidencialidad 22
4.1.2 Integridad 23
4.1.3 Disponibilidad 23
4.2 Hardening 25
4.3 Fases de la ciberseguridad 30
4.4 Metodologías para el Análisis de Riesgos 32
4.5 Sistema de gestión de la Seguridad Informática 38
5. ACTIVOS DE ALTO VALOR Y SISTEMAS DE ALTO IMPACTO 42
5.1. Análisis y Gestión de Riesgos 43
5.2. Visión de conjunto 46
5.3 Método de análisis de riesgos 48
5.4. Proyectos de análisis de riesgos 56
5.5 Plan de seguridad 57
5.6 Análisis y tratamiento de los riesgos 58
6. VULNERABILIDADES DE UN SISTEMA 59
6.1 Vulnerabilidad del día cero 61
6.2 Vulnerabilidades de las Bases de Datos 64
6.3 Vulnerabilidades de las Páginas WEB 66
6.4 Vulnerabilidades en las Redes 69
6.5 Motores de búsqueda de vulnerabilidades 71
7. COMPARACIONES DE METODOLOGIAS 75
7.1 Metodología Octave 75
7.2. Metodología MAGERIT 76

7.3. Metodología MEHARI 77
7.4. Metodología EBIOS 78
7.5. Metodología CORAS 79
7.6. Metodología NIST SP 800 - 30 79
8. ESTRATEGIA PROTECCIÓN DE SEGURIDAD DE LA INFORMACIÓN ..81
8.1. Gestión y control de antivirus y antispam. 81
8.2. Gestión de Actualizaciones Automáticas. 81
8.3. Gestión de Copias de Seguridad. 82
8.4. Gestión de incidentes de seguridad. 82
8.5. Gestión de la Monitorización. 83
8.6. Gestión de Contraseñas. 83
8.7. Gestión de Usuarios. 84
8.8. Gestión de la Configuración (CMDB). 84
8.9. Revisión de Contratos/Mantenimientos/Licencias. 84
8.10. Pruebas de Planes de Contingencia. 85
8.11. Firewall dedicado al entorno de la Organización 85
8.12. Precaución con las conexiones inalámbricas gratuitas o públicas 86
8.13. La información importante es mejor cifrada 86
8.14. Evita acceder a las webs importantes a través de enlaces 86
8.15. Precaución con las descargas de archivos 87
8.16. Sensibilización y capacitación de empleados. 87
9. RECOMENDACIONES 89
CONCLUSIONES 90
REFERENCIAS BIBLIOGRÁFICAS 92
Anexo 1. Tipos de Activos 95
Anexo 2. Amenazas 101
Anexo 3. Salvaguardas 104
Anexo 4. Controles ISO 27000 107

LISTA DE ILUSTRACIONES

Ilustración 1. Pilares Seguridad de la Información 23
Ilustración 2. Pentesting.....25
Ilustración 3. Proceso Hardening.....26
Ilustración 4. Procesos de Ciberseguridad 32
Ilustración 5. ISO 31000 - Marco de trabajo para la gestión de riesgos.....43
Ilustración 6. Ciclo PDCA.....46
Ilustración 7. Proceso de gestión de riesgos (fuente: ISO 31000). 47
Ilustración 8. Elementos del análisis de riesgos potenciales 49
Ilustración 9. El riesgo en función del impacto y la probabilidad. 53
Ilustración 10. Ejemplo de CVE 72
Ilustración 11. Ejemplo de CVE 2 73

LISTA DE TABLAS

Tabla 1. Marco normativo nacional e internacional.....40
Tabla 2. Familia de normas ISO/IEC 27000. 41
Tabla 3. Dimensiones de Valoración 50
Tabla 4. Degradación del Valor.....51
Tabla 5. Probabilidad de Ocurrencia.....52

GLOSARIO

Ciberguerra: Es un ataque cuya finalidad por norma general es política. En este contexto, los ciberdelincuentes recopilan la mayor información posible y datos relevantes donde puedan comprometer, en un futuro cercano, a un partido político o un gobierno[1].

Ciberterrorismo: Esta es otra forma de amenaza común, pero en esta oportunidad, aunque también se intenta reunir el máximo de información, el objetivo es diferente, puesto que es crear un ambiente de terror entre los ciudadanos de una nación o país[2].

Cibercrimen: Es una de las amenazas más comunes y la que más se suele ocasionar en todo tipo de países. A través de esta, los hackers acceden a los sistemas informáticos protegidos e intentan obtener[3].

[1] OBS BUSINESS SCHOOL. [Sitio web]. ¿Qué es ciberseguridad y de qué fases consta? Disponible en https://obsbusiness.school/es/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta
[2] Ibid…
[3] Ibid…

RESUMEN

En el presente trabajo se ha desarrollado un manual con el apoyo de la metodología PHVA (Planear, Hacer, Verificar y Actuar) que permita destacar los pasos que se pueden seguir para la realización de un análisis y diagnóstico de vulnerabilidades cibernéticas en una empresa y de esta forma determinar la solución que logre mitigar los riesgos encontrados, lo anterior teniendo en cuenta que la realización de un hacking ético a una red empresarial es de vital importancia debido a que se pueden validar las diferentes vulnerabilidades presentes en los activos informáticos de la compañía y de esta forma realizar los ajustes necesarios en cada una de las falencias que se logren detectar.

***Palabras Claves**: Hacking, vulnerabilidades, gestión del riesgo*

ABSTRACT

In this work, a manual has been developed with the support of the PHVA methodology (Planning, Doing, Verifying and Acting) that allows highlighting the steps that can be followed to perform an analysis and diagnosis of cyber vulnerabilities in a company and This form will determine the solution that mitigates the risks encountered, the above taking into account that the realization of an ethical hacking to a business network is of vital importance because they can validate the different vulnerabilities present in the company's IT assets and This form makes the necessary adjustments in each of the failures that are detected.

***Keywords**: Hacking, vulnerabilities, risk management*

INTRODUCCIÓN

Desde hace varios años, la palabra ciberseguridad se ha vuelto un modelo entre las compañías, debido a que la informática es una herramienta habitual en las diferentes organizaciones, en donde para mantener los sistemas a salvo hacen falta muchas medidas de seguridad que ayuden a evitar estar expuestos a diferentes riesgos. Cuando se plantea qué es ciberseguridad, hay que mencionar lo que se conoce como seguridad de la tecnología de la información, adicionando un gran número de técnicas y métodos para proteger los sistemas de las organizaciones, así como los diferentes dispositivos o las redes de las organizaciones. Implementando herramientas que son de utilidad con relación a la ciberseguridad, el sistema de una organización será protegido en las ofensivas informáticas, el hackeo o cualquier robo ya se de identidad o de datos. Es así, que para mejorar las medidas es importante dotar el sistema siempre teniendo en cuenta cómo evoluciona este concepto y para así actualizar las nuevas herramientas que van surgiendo para evitar las diferentes amenazas.

En la actualidad los profesionales en seguridad de ISACA (Information Systems Audit and Control Association) indican que la ciberseguridad está definida en la capa de protección donde todos los archivos de información que son manejados en las organizaciones, siendo así, se trabaja para evitar que cualquier tipo de amenazas pongan en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo de las organizaciones colombianas como mundiales.[4]

La ciberseguridad trabaja en robustos sistemas los cuales son preparados de operar antes, durante y después, no solo sirve prevenir, sino que se debe dar la confianza tanto a los clientes y como el mercado, para lograr así reducir los riesgos de exposición ya sea del usuario y los sistemas.

Se sabe que los ataques informáticos se pueden encontrar en cualquier momento y estos siguen evolucionando de forma continua, es decir, que varias

[4] LANZ, Leonela. Openwebinars. Obtenido de https://openwebinars.net/blog/que-es-la-ciberseguridad/. 2018

amenazas que son comunes y habituales en los diferentes sectores del mercado. Lo que esto se refiere a la ciberguerra, el ciberterrorismo y el cibercrimen que van en aumento en el mundo.

1. PLANTEAMIENTO DEL PROBLEMA

Con el paso del tiempo en las organizaciones implementan las nuevas tecnologías de la información dependiendo de las necesidades que se presentan ya sean las páginas web donde pueden mostrar los diferentes servicios que ofrecen, correos institucionales los cuales son manejados por los usuarios de la organización, bases de datos que son manejadas por las diferentes áreas, los software de contabilidad y operacionales, lo que conlleva a las organizaciones invertir en servidores, cableado estructurado, licencias de los diferentes software y actualizaciones que den a lugar, cada uno de estos están ubicados en las diferentes dependencias las cuales son responsables de los diferentes usos que se le den; sin embargo no todas implementan procesos para analizar las vulnerabilidades existentes que pueden ocasionar un incidente cibernético.

Los procesos en la gran mayoría se llevaban de manera manual y estos han realizado un cambio en la sistematización lo cual ha generado un constante miedo hacia la pérdida o filtración de la información, y aunque existen varias metodologías y métodos para la verificación de la información, son la base para poder determinar los riesgos que presentan las organizaciones, es importante contar con un manual que contenga una serie de recomendaciones y pasos más prácticos que permita determinar las vulnerabilidades de seguridad informática presentes en una empresa y a través de las cuales se puede estar expuesto a un ataque cibernético, esto con el fin de cumplir a cabalidad con los tres pilares básicos de la información como son: integridad, confiabilidad y disponibilidad, tanto al interior de la empresa como a todos y cada uno de los colaboradores sin olvidar los clientes externos los cuales proveen información privilegiada para ellos.

Adicional muchas empresas colombianas realizan el manejo de las bases de datos de cada uno de sus clientes, donde se debe evaluar como es el manejo de la información, el modo de transmisión y que niveles de cifrado se utilizan para proteger la información que es remitida por el cliente a la red de la compañía para su respectivo proceso y/o manipulación.

A partir de lo anterior se genera la siguiente pregunta. ¿Cómo un análisis de vulnerabilidades cibernéticas contribuye con el mejoramiento continuó en la evaluación de riesgos de las organizaciones en las PyMES?

2. JUSTIFICACIÓN

Uno de los activos más importantes en las organizaciones es la información, esta información no importar la forma y los tratamientos que se le dé, con el transcurrir de los años lo que se busca es la optimización de los procesos, se comenzó a implementar en las organizaciones la sistematización, logrando efectivamente minimizar los tiempos en las diferentes actividades que se ejecutan en el interior como en el exterior de las organizaciones, partiendo de este posición y con el objeto de satisfacer a los diferentes clientes se utiliza la innovación donde se hace uso del beneficio de los recursos tecnológicos, las organizaciones ha alcanzado al punto incluso de ofrecer los trámites y servicios corporativos en internet, es decir, en sus páginas web, o incluso dentro de la misma organización implementando las redes sociales para acompañar en forma directa los diferentes archivos que se manejen entre cada uno de los otros procesos, donde se coloca el activo principal que es la información, la cual pueda ser de fácil acceso con el fin de cumplir con el objetivo de innovar e impactar a los usuarios.

En el fortalecimiento en la seguridad informática en las organizaciones avanzan de una forma muy rápida ya que también existen personas que se trabajan en el estudio del robo y/o modificación de la información de las organizaciones para poder tener beneficios lucrativos o por interés netamente personales. Partiendo de lo antepuesto, la información es de alcance de los clientes, como de los colaboradores, donde es necesario validar las medidas de seguridad que son necesarias para el tratamiento de la información, debido que se debe mantener en una caja fuerte y una vigilancia constantemente, para evitar que sufra alguna alteración y/o sustracción de la información. Es de conocimiento que los datos que se maneja en las organizaciones son de vital importancia porque son la base fundamental de su funcionamiento, es por eso, que se debe garantizar la seguridad de la forma donde genere la confianza y autenticidad que se necesita.

En la actualidad en Colombia muchas de las empresas cuentan con servicios tecnológicos dentro y fuera de la organización, como es la página web, los correos corporativos, la utilización de las bases de datos en los programas que

manejan las organizaciones, ya sean software contables o los archivos de gran importancia los cuales son la base fundamental para el cumplimiento de la misión y poder así generar la implementación de las nuevas tecnologías y poder generar algunos cambios donde se logre optimizar el trabajo de los colaboradores de las organizaciones. Las compañías de ningún modo han realizado un análisis en la seguridad informática donde puedan garantizar si el manejo de la información es el correcto para poder cumplir con los pilares de la información que son la confidencialidad, la integridad y la disponibilidad, donde se beneficia los diferentes clientes que utilizan los diferentes servicios que ofrece la organización.

Las metodologías en la realización de los diferentes análisis de riesgos que conforma el sistema de gestión de seguridad de la información – SGSI en las compañías, donde se realiza los escaneos de vulnerabilidades se utiliza una serie de modelos y procesos para tal fin. Uno de los objetivos de las metodologías del análisis de riesgos es la planificación de la reducción de riesgos, prevención de accidentes, visualización y detección de las debilidades existentes en los sistemas y ayuda en la toma de las mejores decisiones en materia de seguridad de la información[5]. Con este manual lo que se pretende lograr es generar una guía y las diferentes alternativas que existen en la generación de análisis de acuerdo con las necesidades de la organización basándose en las diferentes metodologías que existen donde se relacionas cada una de las ventajas que tienen.

[5] NOVOA, Helen. RODRIGUEZ, Claudia. Metodologías para el análisis de riesgos en los SGSI. 2015. Vol. 9, p. 3

3. OBJETIVOS

3.1 Objetivo General

Evaluar las vulnerabilidades cibernéticas que afectan la gestión del riesgo en las PyMES.

3.2 Objetivos Específicos

- Establecer los recursos necesarios en activos de alto valor y sistemas de alto impacto que requieren mayores niveles de protección.
- Examinar las vulnerabilidades cibernéticas dentro de las infraestructuras tecnológicas y de comunicación en las PyMES.
- Comparar las metodologías más utilizadas en el análisis y gestión de riesgos en los sistemas de información en las PyMES.
- Diseñar una estrategia de protección de seguridad que minimice el impacto de los diferentes ataques y riesgos cibernéticos, implementando medidas de seguridad apropiadas y acordes con el riesgo económico y social de las PyMES.

4. MARCO CONCEPTUAL Y TEÓRICO

En el aumento acelerado del uso de la tecnología en vida del ser humano y en las organizaciones, la mayor dependencia de los sistemas de información se hace que la seguridad de la información juegue un rol muy importante en las actividades diarias.

Por otra parte, el acceso fácil a las herramientas para determinar las vulnerabilidades de cualquier sistema hace que las personas malintencionadas y muchas veces sin tener mayor conocimiento sobre redes desean tener acceso a la información valiosa que tienen las organizaciones privadas o públicas haciendo que están muestren los problemas en su desempeño diario ocasionando daños en la red, en los equipos y lo que es más importante causando pérdidas económicas en la compañía.

Una de las causas de mayor importancia para la existencia de la seguridad en redes y la información es el esfuerzo por mantenerse un paso adelante de los personas malintencionados o llamados hackers. Los profesionales en la seguridad informática quien intenta prevenir ataques mermando los efectos de los ataques en tiempo real.

Ciberataques en Colombia

En Colombia, el actor más reconocido es el grupo activista Anonymous, el cual ha realizado un sin número de ataques, entre los cuales se encuentran ataques de DDos contra páginas de entidades gubernamentales. El día 11 de abril de 2011 fue atacada la página web del Ministerio del Interior y de Justicia de Colombia, como protesta por el proyecto de ley que impulsó este ministerio, el cual buscaba penalizar la piratería informática; dicha iniciativa era conocida en la red como Ley Lleras. Tres días después, fue atacada la página del Senado de la República de Colombia y el portal web del programa Gobierno en Línea.

Posteriormente, el 15 de abril del mismo año, el objetivo fue la página web de la Presidencia de República[6].

El 20 de septiembre de 2012, el Ministerio de Defensa Nacional, el Grupo de Respuestas a Incidentes de Seguridad Cibernética (ColCERT), con el apoyo del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA) y el Departamento de Ingeniería de Sistemas y Computación, y la Dirección de Tecnologías de Información (DTI) de la Universidad de los Andes, realizaron el primer simulacro nacional de incidentes cibernéticos, con el fin de fortalecer las capacidades del Estado Colombiano en la prevención, la detección y mitigación de los efectos de un ataque cibernético de gran escala[7].

En Colombia, el Centro Cibernético Policial (CCP), durante el año 2013, atendió en total de 1.647 ataques cibernéticos, la mayoría de estos ataques fueron dirigidos a ciudadanos particulares (62%), el 21% a entidades del sector financiero y el 17% restante a entidades del gobierno, comunicaciones, energía, salud y educación[8].

Dicho centro logró establecer tres tendencias principales en materia de delitos cibernéticos. La de mayor uso es la utilización de códigos maliciosos Phishing, y robo de información que afecta a los usuarios y entidades del sector financiero, esto gracias a una débil cultura de seguridad cibernética. La segunda tendencia, es la fuga o robo de información, interceptación de datos y uso abusivo de los sistemas. Y la tercera, se presenta gracias al uso masivo de internet por parte de organizaciones y usuarios, los cuales se vieron involucrados en casos de cobro masivo ilegal de dinero (por ejemplo, pirámides cibernéticas), el uso de divisas virtuales como mecanismo para lavar dinero y negocios ilícitos que involucran el tráfico de armas, las drogas, la pornografía infantil, etcétera[9].

---

[6] REUTERS citado por NIÑO, Yamith. Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo pymes. 2015. p 17

[7] Universidad de los Andes. Simulacro de ataques a infraestructuras nacionales. 2012.

[8] Symantec Corporation. Contexto Latinoamericano - tendencias de ciberseguridad en América Latina y el Caribe. 2014

[9] Organización de los Estados Americanos. Estrategia de seguridad cibernética. 2004

En los últimos años, las pequeñas y medianas empresas han sido víctimas de ataques cibernéticos mediante la interceptación de comunicaciones establecidas con sus proveedores y clientes[10]. En estas organizaciones afrontan una gran cantidad de amenazas que va saliendo y evolucionado; por lo anterior se requiere establecer diferentes medidas que puedan dar cumplimiento de los estándares de seguridad que se establecen en el país; no se puede olvidad evaluar en implementar el concepto de ciberseguridad en las organizaciones, esto permite a la alta dirección poder identificar y tratar los riesgos encontrados como parte de la gestión organizacional.

4.1 Principios de la seguridad de la información

La seguridad de la información se basa en los tres principios fundamentales sin ellos proteger los datos importantes de las compañías sería una pérdida de tiempo y sobre todo se pone en riesgo la red, los activos, la información y el normal funcionamiento de la entidad.

4.1.1 Confidencialidad

Esta se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, basado en este principio, las herramientas de seguridad informática deben proteger los sistemas de invasores y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados[11].

[10] Policía Nacional. Boletín de análisis en Ciberseguridad Pyme. 2015

[11] González, D. F. El riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas BASC. 2014. p 13.

4.1.2 Integridad

Esta se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático, basado en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es transcendental en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información[12].

4.1.3 Disponibilidad

Esta se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático, basado en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromisos con el usuario, son prestar servicio permanente[13].

Ilustración 1. Pilares Seguridad de la Información

[12] González, D. F. Op. cit, p 13.
[13] Ibid., p 11 y 12

Con lo anterior y para poder garantizar los principios de la seguridad, se realizan las diferentes pruebas de pentesting o de penetración, este proceso donde se comprueba el nivel de seguridad que tiene el sistema informático de la organización realizando ataques con el fin de hallar las posibles vulnerabilidades que una persona ajena a la organización puede valer para robar, controlar y/o manipular la información. Estas pruebas son especializadas en realizar a los sistemas los cuales son implementados y próximos a salir a producción.

Existen varios tipos de Pentesting en las actividades comerciales, pero los más comunes son los siguientes:

- Prueba de caja Negra (Black-Box): El equipo de pruebas no tiene información por anticipado sobre la red de la compañía, solo se cuenta con una dirección IP de un sitio web o ftp, el objetivo de esta prueba es tratar de irrumpir en la página web o servidor con el fin de sacar información como puertos de conexión TCP/IP abiertos, atacando el servicio de forma maliciosa[14].
- Prueba caja Blanca (White-Box): El equipo de pruebas cuenta con acceso para evaluar las redes, servidores, equipos finales y aplicaciones web, además cuenta con los diagramas de conexión para evaluar con total conocimiento cualquier equipo de la compañía, el objetivo solo va encaminado a evaluar equipos específicos o servicios con el fin de revisar el nivel se seguridad implementado[15].
- Prueba de caja Gris (Grey-Box): El equipo de pruebas tiene información parcial de los equipos de la compañía y tiene como objetivo simular un ataque de un empleado inconforme, se debe dotar al equipo de trabajo de los privilegios necesarios para realizar esta prueba[16].

[14] Barreto, J. H. Diseño de manual de diagnóstico y prevención de Vulnerabilidades en redes de datos para pymes. 2018. p 18.
[15] Ibid., p 18
[16] Ibid.., p 18

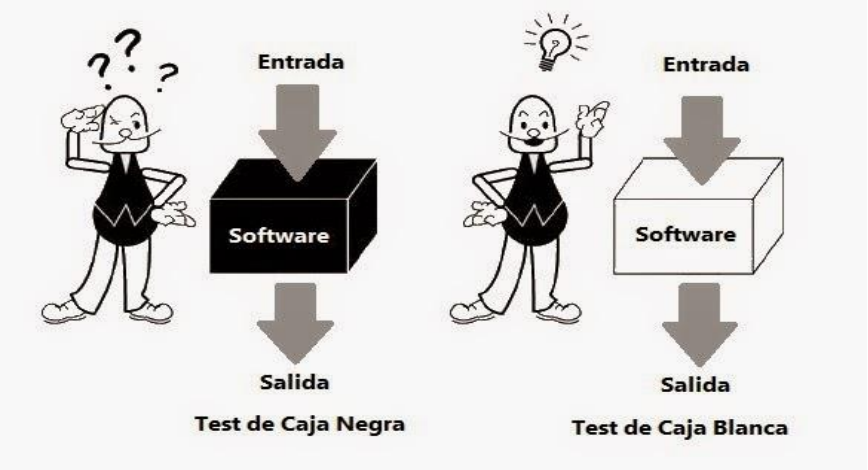


Ilustración 2. Pentesting

4.2 Hardening

Se basa en la configuración robusta a nivel de seguridad con el fin de impedir los ataques informáticos, en la actualidad el software que se instala viene con configuraciones por defecto, abren los puertos innecesarios automáticamente, genera contraseñas genéricas, una multitud de parámetros los cuales no son controlados a simple vista, sino que se instala y se configura por defecto poniendo en riesgo el sistema y posteriormente la información, como medida de protección es necesario realizar un proceso de configuración personalizada (hardening) que busque la protección de un sistema de información, este proceso como se indica es personalizado y la entidad debe documentar y especificar bien las funciones de cada empleado con el fin de bloquear lo que no está permitido y dar acceso exclusivamente al rol a los trabajadores, esto además optimiza el recurso humano para que se enfatice en su trabajo y no distraiga su atención en otros temas relacionados con el sistema[17].

[17] Ibid…, p 17

Ilustración 3. Proceso Hardening

Para la preparación del proceso hardening se debe realizar y tener en cuenta revisiones técnicas que a continuación se mencionan:

- Línea base de seguridad para usuarios: esta configuración tiene como objetivo asegurar el equipo con bloqueos físicos como la desconexión de cables, de puertos de medios extraíbles USB y CD, adicional configuración del equipo para denegar el acceso a la consola de comandos, con el fin de evitar que el usuario manipule comandos que puedan afectar la red[18].
- Línea base de seguridad para usuarios VIP: Existen usuarios privilegiados en función de su rol dentro de la compañía. Estos usuarios tienen requisitos de seguridad, privacidad y confidencialidad diferentes de acuerdo a la información a la que acceden[19].
- Línea base de seguridad para servidores: Bastionado de sistemas depende del rol que desempeñan si es un directorio activo, servidor web, servidor de bases de datos[20].

La definición y distribución de las diferentes directivas que son necesarias para el aseguramiento de los sistemas operativos, se debe realizar mediante los estándares de seguridad, es necesario que el especialista de seguridad informática tenga el conocimiento suficiente en las limitaciones. Los aportes que se tienen en cuenta como el comando TELNET para una conexión insegura dado la alta posibilidad de hurto de credenciales o usuarios para el ingreso a los

[18] Ibid…., p 18
[19] Ibid….., p 18
[20] Ibid….., p 18

sistemas de la organización, este protocolo se utiliza para realizar conexiones a los equipos remotos con el fin de dirigir mediante consola las funcionalidades de cada uno de los equipos, no obstante, el riesgo informático bastante alto ya que el tráfico de las credenciales o datos no se transportan cifradamente sino por el contrario viaja en texto plano alcanzando así la posibilidad de un atacante tenga las credenciales por medio de un sniffing o las herramientas de análisis de tráfico poniendo en riesgo la organización lo que genera un alto impacto de indisponibilidad e integridad de la información que se maneja internamente.

Para tener claro y determinar los pilares fundamentales de la seguridad informática se deben conocer lo siguientes puntos:

- Confidencialidad: consiste en proteger la información contra lectura no autorizada incluye específicamente piezas individuales que pueden inferir en otros elementos de la información[21].
- Integridad: consiste en tratar la información de manera confiable, que por ningún motivo la información puede ser dañada y manipulada sin previo aviso o manipulación por entes no propietarios[22].
- Autenticidad: Garantizar que el usuario X es el quien dice ser, se deben implementar mecanismos de autenticación en los equipos con el fin de evitar suplantaciones[23].
- SSH: Secure Shell interprete de órdenes seguras, este protocolo mediante cifrado de conexión permite que el atacante no interprete las credenciales enviadas a un sistema remoto protegiendo así el acceso de forma segura.
- Cifrado: trasformar la información por letras, números y símbolos, con el fin ocultar y asegurar la confidencialidad y autenticidad de la información ante personas ajenas, el cifrado se utiliza para guardar y ocultar los mensajes privados enviados por la red informática

[21] Excellence, I. ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? 2017
[22] Ibid.,2017
[23] Ibid..,2017

- ACL: Listas de control de acceso o firewall, estas listas son utilizadas para permitir o denegar tráfico entrante en una red de área local con el fin de bloquear acceso no permitidos por la entidad.
- Política Usuario Local y dominio: determinar el perfil del usuario en un equipo local tales como permiso de ejecución, permisos de configuración, permisos de acceso.
- Controles de seguridad: a nivel tecnológico se dividen en tres aspectos físicos, técnicos y administrativos.
- Virus informativos: software que tiene por objetivo alterar el normal funcionamiento de un sistema sin el conocimiento o permiso del usuario
- Riesgos, se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos.
- Vulnerabilidades: es un estado viciado en un sistema informático que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.
- Pruebas de penetración: es un a practica para poner a prueba un sistema de información con el fin de encontrar vulnerabilidades que pueda explorar un delincuente informático.
- LSOF - (List Open Files): Esta herramienta forense y de diagnóstico específica de Unix lista información acerca de cualquiera archivo abierto por procesos que estén actualmente ejecutándose en el sistema. También puede listar sockets de comunicaciones abiertos por cada proceso[24].
- Hunt: Un "packet sniffer" y un intruso en conexiones "connection intrusion" avanzado para Linux. Hunt puede observar varias conexiones de TCP, entrometerse en ellas, o reiniciarlas. Hunt fue hecho para ser usado sobre ethernet, y tiene mecanismos activos para olfatear (sniff) conexiones en redes con los switches. Las características avanzadas incluyen "ARP relaying" selectivo y sincronización de conexión luego de ataques[25].

[24] Rodríguez, A. M. Análisis y diagnóstico de la seguridad informática de Indeportes Boyacá. 2014. p 32
[25] Ibid., p 32

- Fragroute: La peor pesadilla de los IDS.Fragroute intercepta, modifica, y reescribe el tráfico de salida, implementando la mayoría de los ataques descriptos en el "IDS Evasion paper" de Secure Networks. Entre sus características, se encuentra un lenguaje de reglas simple para retrasar, duplicar, descartar, fragmentar, superponer, imprimir, reordenar, segmentar, especificar source-routing y otras operaciones más en todos los paquetes salientes destinados a un host en particular, con un mínimo soporte de comportamiento aleatorio o probabilístico[26].
- Firewalk: traceroute avanzado. Firewalk emplea técnicas similares a las de traceroute para analizar las respuestas a paquetes de IP para determinar mapas de redes y filtros de listas de control de acceso (ACL) empleadas por gateways[27].

El manejo de las herramientas es fundamental para las diferentes soluciones que se pueden brindar para la seguridad donde es necesario en las organizaciones. Donde no se puede dejar de lado que estas soluciones son una parte de la seguridad para estar seguros de los diferentes ataques que puedan realizar.

- La protección contra el código malicioso malware: Esta herramienta es conocida como antivirus, este nivel de seguridad es necesaria en todas las organizaciones, donde no se tiene en cuenta ni la actividad o el tamaño de la misma, es transcendental ir más allá de los sistemas informáticos, sitios de trabajo o los mismos servidores, es reunir cada uno de los aspectos que se corresponden con la movilidad. La existencia de distintos tipos de malware y su progreso donde se convierten en las amenazas más complicadas de trabajar para las personas encargadas en la seguridad de las organizaciones.
- La protección antifraude o pishing: Esta herramienta es de gran importancia ya que el engaño, se ha transformado en los conocimientos más usadas en la red, tanto para infectar los dispositivos no solo de la organización sino personales, como para obtener los datos de los cada

[26] Ibid.., p 32
[27] Ibid…, p 32

uno de los usuarios de las organizaciones. Aquí no existe una herramienta que ayude a combatir las diferentes amenazas, se debe que contar más con el sentido común de los operadores y/o desconfiar de lugares sospechosos en todo momento que se navegan.

- Protección de comunicaciones: Los procedimientos se delega para proteger a las organizaciones de un indeterminado volumen de amenazas, como son los ataques de DDS o denegación de servicios, accesos no autorizados o la intercepción de las comunicaciones en la organización. Así mismo, se tiene en cuenta las amenazas no solo se encuentran desde Internet, sino que también internamente en las organizaciones, para ello la protección de cada una de las comunicaciones es fundamental cuando existen varias sedes en diferentes partes del país o del mundo.

4.3 Fases de la ciberseguridad

En la protección de los diferentes peligros que existen en la actualidad involucra los diferentes procesos de ciberseguridad que se sostengan su efectividad y así lograr hacerlo, se debe identificar cada una de las fases en las que se debe aplicar. Este proceso se divide en tres fases:

- Prevención: Lo que reduce en gran medida el margen de riesgo es actuar de forma temprana e informar de todo lo que puede ocurrir al sistema de la organización, donde se determina las posibles amenazas y cuáles serán las medidas de prevención y reacción en caso de afectarse por una de ellas, esto nos permite estar preparados. Es fundamental que los colaboradores de la organización tengan conocimientos básicos sobre ciberseguridad. Se debe conocer las diferentes herramientas que se utilizan y cómo garantizar su máximo nivel de seguridad para que no se cometan errores donde abran el camino de los hackers[28].

[28] Universidad de Barcelona. ¿Qué es ciberseguridad y de qué fases consta?. 2018

- Localización: Posteriormente de prevenir, en el caso de existir algún tipo de problema, se genera la localización dónde se tiene el problema. Para ello la mejor herramienta es disponer de un antivirus potente que ayude a detectar el ataque en tiempo real y así concentrarse de inmediato. Localizar un ataque o una infección no es tan fácil como pueda considerar, dado que los hackers son conscientes del uso de los antivirus existentes en el mercado y lo que hacen es trabajar de manera que sus ataques puedan pasar desapercibidos por estos antivirus. Cualquiera sea el caso, desde el momento en el que se produce el golpe hasta que la organización lo detecta, pueden pasar aproximadamente 100 días. Para lograr reducir en la medida de lo posible este inconveniente, hay concentrarse en dos aspectos: gestionar las vulnerabilidades del sistema y por otro llevar a cabo una monitorización de forma continua en la organización[29].
- Reacción: Una vez sea localizado la amenaza, se tendrá que dar una respuesta técnica sobre la misma y para ello es primordial seguir los siguientes pasos. Se inicia con la desconexión de los equipos de la red y seguidamente se instala un antivirus que pueda satisfacer las necesidades o actualización del que se tiene. Posteriormente, se lleva a cabo un análisis sobre el sistema y se genera los cambios en las contraseñas de todos los usuarios. Para finalizar, es crucial realizar una limpieza a fondo del sistema para comprobar que ya no existe ningún tipo de peligro. En el caso de que nos hayan robado información confidencial, también se debe proceder de la manera pertinente para comunicarlo a los usuarios afectados y así elevar lo ocurrido a una situación de delito informático[30].

[29] Ibid., 2018
[30] Ibid.., 2018

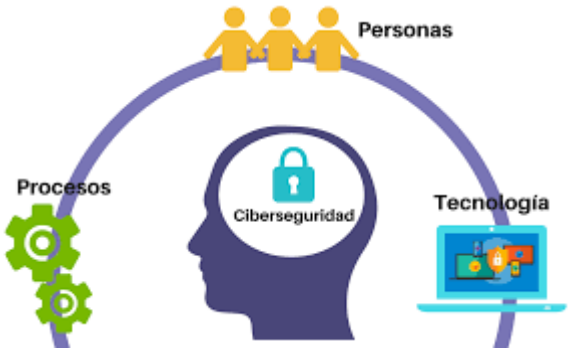


Ilustración 4. Procesos de Ciberseguridad

4.4 Metodologías para el Análisis de Riesgos

La seguridad informática existe varias metodologías de análisis de riesgos dentro de las que resaltan son las siguientes: Octave, Magerit, Mehari, NIST SP 800:30 y Coras, Cramm y Ebios

- **Octave (Operationally Critical Threat, As-set, and Vulnerability Evaluation).**

Es una de las metodologías de análisis de riesgos más utilizada por las empresas. Esta describe un conjunto de criterios para desarrollar métodos que se adhieran a guías específicas de evaluación y administración de riesgos. Octave evalúa los riesgos de seguridad de la información y propone un plan de mitigación de estos dentro de una organización. Sus objetivos se encuentran enfocados básicamente en concientizar a la organización en cuanto a que la seguridad informática no es un asunto solamente técnico, y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos. Este tipo de metodología realiza diversos procesos. Inicia con una evaluación de los activos relacionados con la información, para luego asignarles un valor estimado para la organización; de esta manera, la metodología Octave analiza y estudia la infraestructura de la información, definiendo así los elementos más importantes para la empresa. Es una técnica de organización, proyección, clasificación y consultoría importante

en seguridad de la información establecida en el riesgo; esta técnica logra su misión en tres procesos: auto dirigido, flexible y evolucionado, que, a su vez, se desarrolla en tres fases: perfiles de amenazas basados en activos, identificación de vulnerabilidades de la infraestructura y desarrollo de estrategia y planes de seguridad. La metodología Octave orienta a la organización para que dirija y gestione sus evaluaciones de riesgo, tome decisiones basadas en sus riesgos, proteja los activos críticos de información y comunique de forma efectiva la información clave de seguridad, para que, así, obtenga los siguientes beneficios: permitir la identificación de riesgos de la seguridad que puedan impedir la consecución del objetivo de la organización; enseñar a evaluar los riesgos de la seguridad de la información; crear una estrategia de protección con el objetivo de reducir los riesgos de seguridad de la información prioritaria y ayudar a la organización a cumplir regulaciones de la seguridad de la información[31]..

- **Magerit.**

Es la metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración Electrónica. En la introducción de esa metodología sobresalen dos objetivos principales, uno de los cuales es estudiar los riesgos que soporta un sistema de información y el entorno asociado a este, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, en una primera aproximación que se atiene a la aceptación habitual del término, y otro relacionado con recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir impedir, reducir o controlar los riesgos investigados. Siguiendo la terminología de la norma ISO 31000, Estándar sobre principios y directrices para la gestión de riesgo, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos"; es decir, Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Magerit define la seguridad como "la capacidad de las redes o de los sistemas de información para

[31] Novoa, H. A. Metodologías para el análisis de riesgos en los SGSI. 2015. p 75

resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles". Los principales elementos para el análisis de riesgos, según Magerit son: activo, amenaza, vulnerabilidades, impacto, riesgo y salvaguardas (funciones, servicios y mecanismos)[32].

- **Mehari.**

Método Armonizado de Análisis de Riesgos. Esta metodología fue propuesta y desarrollada por el Club Francés de la Seguridad de la Información CLUSIF en el año 1996; es de acceso público y para todo tipo de organizaciones. Se diseñó inicialmente y se actualiza continuamente para ayudar a los CISO (Chief Information Security Officers) en la gestión de las actividades de la seguridad informática, pero también está concebida para auditores CIO o gestores de riesgos. Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgo, evaluando cuantitativamente, de acuerdo con la situación de la organización, dónde se requiere el análisis; acopla lo objetivos estratégicos existentes con los nuevos métodos de funcionamiento de la empresa mediante una política de seguridad y mantenimiento de los riesgos a un nivel convenido. Mehari propone un módulo para analizar los intereses implicados por la seguridad y un método de análisis de riesgos con herramientas de apoyo. El principal objetivo de Mehari es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos ISO/IEC 27005:2008, por medio de un conjunto de herramientas y elementos necesarios para su implementación. Los aspectos fundamentales de esta metodología son: diseño de un modelo de riesgo, evaluación de la eficiencia de las políticas de seguridad previamente planteadas en la organización y capacidad para valorar y simular los niveles de riesgo. Sus archivos e instrumentos oficiales hacen énfasis en un marco

[32] Ibid., p 75

metodológico y una base de conocimientos con la finalidad de investigar y realizar un análisis de los diferentes inconvenientes y falencias que se presentan, poner en consideración las vulnerabilidades en los sistemas de información, dar solución a las mismas, disminuir y controlar los riesgos y supervisar la seguridad de la información. Con Mehari se detectan vulnerabilidades mediante auditorías, se analizan situaciones de riesgo y se razonan sus contextos[33].

- **NIST SP 800 – 3.**

Esta guía que plantea ciertas recomendaciones y actividades para una realizar una gestión de riesgos como parte de la seguridad de la información que se debe realizar en una organización; por consiguiente, es necesario el apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos planteados finalicen con éxito. La Metodología NIST SP 800-30 se compone por 9 pasos o fases para el análisis de riesgo:

- Paso 1: Caracterización del sistema.
- Paso 2: Identificación de amenaza.
- Paso 3: Identificación de vulnerabilidades.
- Paso 4: Control de análisis.
- Paso 5: Determinación del riesgo.
- Paso 6: Análisis de impacto.
- Paso 7: Determinación del riesgo.
- Paso 8: Recomendaciones de control.
- Paso 9: Documentación de resultados.

Suministra una base para que proceso desarrolle un programa efectivo de la evaluación de la gestión de riesgos, esta debe contener las definiciones como cada uno de los puntos a desarrollo para que el programa sea eficaz en la gestión de riesgos y la orientación práctica necesaria para mitigar y evaluar cada uno los riesgos que se identifican dentro de los sistemas de TI. El objetivo principal es ayudar a las diferentes organizaciones poder gestionar de una mejor manera los riesgos con un proceso de cuatro fases como lo es evaluación, mitigación,

[33] Ibid.., p 76

análisis y evaluación de los riesgos. NIST se enfatiza que la gestión de riesgos en proyectos de TI donde alcanza niveles satisfactorios en los hardware, software, Base de Datos, redes y las telecomunicaciones, pues que la estructura establece los diferentes criterios de seguridad, donde los más comunes son la confidencialidad, integridad y disponibilidad[34].

Por lo anterior, son la base para generar los análisis y así valorar la materialización de las amenazas e impactos sobre cada uno de los elementos de TI. No obstante, esta metodología por ser tan robusta es un limitante para la aplicación en pequeñas empresas con altas limitaciones de talento humano.

- **Coras – Construct a Platform for Risk Analysis of Security Critical Systems**

Consultative Objetive Risk Analysis System es un proyecto desarrollado desde el año 2001 por Sintef, un grupo de investigadores noruego financiado por organizaciones del sector público y privado, cuya misión es proporcionar un marco de trabajo encaminado a sistemas en los que la seguridad es crítica. Su aplicación permite la detección de fallas de seguridad, inconsistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad, exploradas en siete etapas: presentación, análisis de alto nivel, aprobación, identificación de riesgos, estimación de riesgo, evaluación de riesgo y tratamiento del riesgo. Se trata de una técnica que es muy útil para equipos heterogéneos que intenten identificar vulnerabilidades y amenazas a sus activos de valor. Esta metodología suministra un método basado en modelos, acompañado específicamente de los siguientes componentes:

- Una metodología de análisis de riesgos basado en la elaboración de modelos.
- Un lenguaje gráfico basado en UML (Unified Modelling Language).

[34] Ibid…, p 77

- Un editor gráfico para soportar la elaboración de modelos (Microsoft Visio).
- Una biblioteca de casos reutilizables.
- Una herramienta de gestión de casos (gestión y reutilización de casos).
- Representación textual basada en XML (eXten-sible Mark-up Language).
- Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos.

El método Coras provee un editor gráfico en el cual se diseñan los modelos de lenguaje basados en Microsoft Visio, una librería de casos reutilizables, un objeto de gestión de casos y un formato general de informes, el cual facilita la comunicación entre diferentes partes del proceso de análisis de riesgo[35].

- **Cramm (CCTA Risk Analysis and Management Method)**

Es una metodología de análisis de riesgos, que fue desarrollada por el Central Communication and Telecommunication Agency (CCTA) del gobierno del Reino Unido, por lo general, esta metodología está dirigida en Europa y a grandes industrias u organizaciones gubernamentales. De igual manera, Cramm divide en esta metodología en tres etapas: la primera establece los objetivos de seguridad; la segunda realiza un análisis de riesgos y por último se identifica y se selección los salvaguardas. Cramm define una Metodología para el análisis y gestión de riesgos enfocada a ofrecer confidencialidad, integridad y disponibilidad de los sistemas de información mediante el uso de una evaluación mixta.

- **Ebios - Expresión de las necesidades e identificación de los objetivos de seguridad**

Esta metodología francesa realiza un análisis y de gestión de riesgos en la seguridad de sistemas de información donde comprende un conjunto de guías y

[35] Ibid…., p 78

herramientas de código libre, la cual está enfocada a gestores del riesgo de TI. Esta metodología se desdobla mediante cinco (5) fases:

- Fase 1: estudio del contexto.
- Fase 2: estudio de los eventos peligrosos.
- Fase 3: estudio de los escenarios de amenazas.
- Fase 4: estudio de los riesgos.
- Fase 5: estudio de las medidas de seguridad, Caso práctico.

Esta herramienta es muy completa la cual permite evaluar y abordar los diferentes riesgos relacionados con la seguridad informática promoviendo una eficaz comunicación en cada una de las áreas de la organización y entre sus socios, dando cumpliendo a cada uno de los estándares de la ISO 27001, 27005 y 31000 para la gestión de riesgos y brindando las justificaciones necesarias para la toma de decisiones (descripciones precisas, retos estratégicos, riesgos detallados con su impacto en el organismo objetivos y requerimientos de seguridad explícitos). Ebios es una verdadera herramienta de negociación y arbitraje[36].

4.5 Sistema de gestión de la Seguridad Informática

La información es uno de los activos más importantes de las organizaciones. Su inconstancia da cuenta de los procesos que constituyen el ser y hacer de las actividades y funcionamiento organizacional. Es así, que la estructura de datos de la información procede de diferentes fuentes y transitan a través de las diferentes bases y/o redes cibernéticas que existen, convirtiendo las velocidades y espacialidades de su acceso y utilidad, pero a su vez, se expone a niveles de riesgos y amenazas que deben ser evaluados y controlados tanto de manera técnica y gerencial para así controlar de manera eficaz los niveles de vulnerabilidad que pueden existir.

[36] Ibid….., p 78

La gestión en seguridad informática, gira en torno de los tres ejes que son la disponibilidad, la integridad y la confiabilidad de los datos. La posición de una organización o empresa está ligada a su posibilidad de manejar de manera eficiente y eficaz los datos para disponer de ellos cuando y donde se requieran, los datos que a su vez sean completos y verificables, además no deben estar a disposición de personal no autorizado por el área o la organización. Los factores que evalúan los procesos de gestión de seguridad informática y que se convierten en una de las mejores inversiones en las organizaciones, inversión que se traduce en la certificación internacional y también en una imagen de confiabilidad para los clientes.

El Sistema de Gestión de Seguridad Informática es un proceso sistemático, protocolizado y manejado por los miembros de la organización que permite la confiabilidad, integridad y disponibilidad de la información. El SGSI ha venido implementando desde los comienzos de la información masiva, sin embargo, fue en la década de los años 90 que se dio inició al diseño de estrategias y metodologías para su implementación, siendo Gran Bretaña y los Estados Unidos líderes.

Entidades Normalizadoras	
ISO / IEC	International Organization for Standarization. Organización encargada de crear normas de estandarización internacional. La ISO/IEC es un marco internacional de las prácticas de seguridad informática reconociendo la información como un activo de gran valor para las empresas
ICONTEC	Instituto Colombiano de normas técnicas y certificación. Es el organismo que emite las certificaciones de calidad en Colombia.
CEN/CENELAC	Comité europeo de normalización electrónica que junto a la ETSI produce normas aplicables a nivel mundial en torno a las TIC
BSI	British Standards Institution (BSI), institución británica encargada de la creación de normas para la estandarización

	de procesos, centra sus actividades en la certificación, auditoria y formación de normas. Es una entidad colaboradora de la ISO y proveedora de normas.

Tabla 1. Marco normativo nacional e internacional

La norma ISO/IEC es una serie de normas entorno al Sistema de Gestión de Seguridad Informática donde se definen términos procesos de implementación y evaluación. Los rangos de numeración van de 27000 a 27019 y de 27030 a 27044.

Norma ISO/IEC	Fecha	Contenido
27000	2008	Términos y definiciones que estandarizan el vocabulario de la serie.
27001	2005, 2013 ultima Actualización	Sistema de Gestión de Seguridad de la Información. SGSI. Norma certificable.
27002	2010	Guía de implementación de SGSI
27004	2009	Especifica métricas y técnicas de medidas aplicables para determinar la eficacia del SGSI
27005	2008, Revisada 2011	Diseñada para ayudar a la aplicación de la seguridad informática desde un enfoque de gestión de riesgos.
27006	2007	Requisitos para la acreditación de entidades de auditoria y certificación.
27007	2011	Guía de auditoria.
27011	2008	Implementación del SGSI en el sector de telecomunicaciones.
27017	2015	Guía de seguridad para Cloud Computing, (computación en la nube).
27031	2010	Guía de continuidad de negocio en cuanto a tecnologías de información y comunicaciones.
27034	2012	Guía de seguridad en aplicaciones

27035	2011	Guía de gestión de incidentes de seguridad
27799	2008	Estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (Salud informática).

Tabla 2. Familia de normas ISO/IEC 27000.

5. ACTIVOS DE ALTO VALOR Y SISTEMAS DE ALTO IMPACTO

La realización de un inventario y clasificación de los activos de alto valor se hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de las organizaciones, es así que se utilizará la metodología Magerit en la cual se explicará los siguientes temas a profundidad

- Inventario de activos: todos los activos deben estar claramente identificados y la organización debe elaborar y mantener un inventario de los mismos.
- Propiedad de los activos: los activos de información del inventario deben tener un propietario.
- Clasificación de la información: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- Etiquetado y manipulado de la información: Se debería 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.

El inventario de activos de información de las organizaciones debe especificar para cada activo:

- Información básica del activo (nombre, observaciones, proceso, entre otras).
- El nivel de clasificación de la información.
- Información relacionada con su ubicación, tanto física como electrónica.
- Su propietario y su custodio.
- Los usuarios y derechos de acceso.

5.1. Análisis y Gestión de Riesgos

La metodología Magerit se basa en la terminología de la normativa ISO 31000 a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información[37].

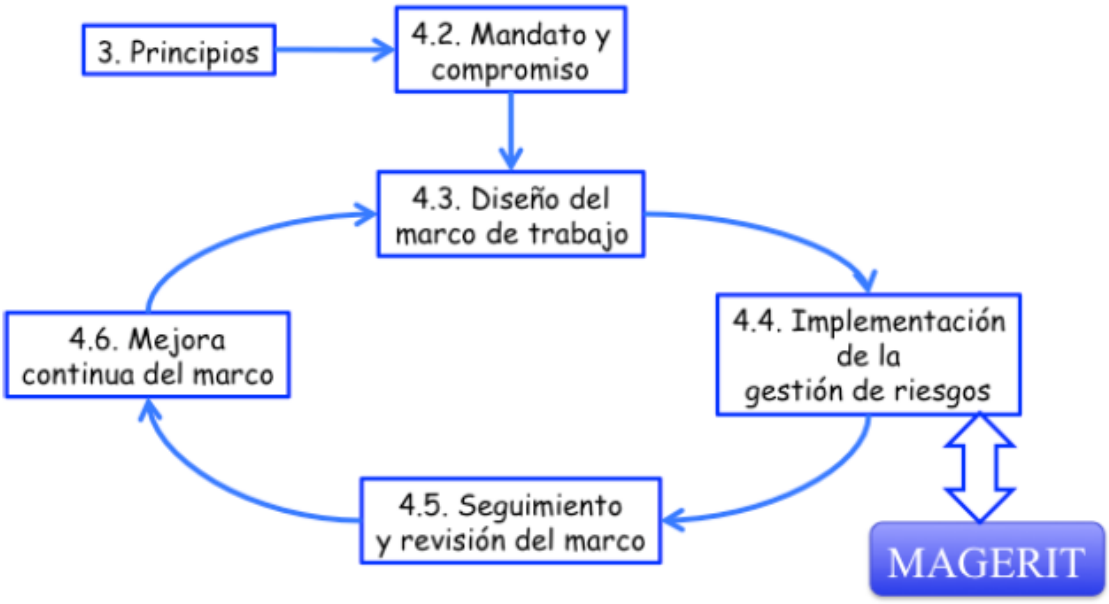


Ilustración 5. ISO 31000 - Marco de trabajo para la gestión de riesgos.

Con esta metodología de Magerit lo que se pretende conseguir los objetivos:

Directos:

- 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).

[37] Amutio Gómez, M. A., Candau, J., & Mañas, J. A. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I, II y III. 2012. p 7

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso[38].

Lo que se busca con la estandarización de los informes que almacenan los diferentes hallazgos y así poder analizar cada una de las conclusiones de las actividades que se realicen en la gestión de riesgos:

- Modelo de valor.
- Mapa de riesgos.
- Declaración de aplicabilidad.
- Evaluación de salvaguardas.
- Estado de riesgo.
- Informe de insuficiencias.
- Cumplimiento de normativa.
- Plan de seguridad.

El análisis de riesgos accede a establecer el cómo es, cuánto vale y cómo se encuentra protegido el sistema. La coordinación de los objetivos, estrategia y de la política de la organización, el tratamiento de los riesgos permite elaborar un plan de seguridad que se encuentre implantado y operado, a lo cual, se logre cada uno de los objetivos presentados con el nivel de riesgo que acepta la Dirección de la organización. La unión de estas actividades se le designa el nombre de "*Proceso de Gestión de Riesgos*".

La implantación de las diferentes medidas de seguridad que es necesario que sean organizadas y que la participación del personal que trabaja con los sistemas de información de la Organización. Dicho personal será responsable de las operaciones, de la resistencia ante incidencias y del monitorio del sistema para

[38] Ibid., p 8

poder determinar si satisface con eficiencia y eficacia de los objetivos propuestos por la organización.

El esquema de trabajo es monótono ya que los sistemas de información escasamente son modificables; es así, que la evolución de estos sistemas se realiza con la inserción de nuevos activas para la organización como en el entorno de nuevas amenazas, lo cual exige que se realice una revisión habitual en la que se aprende de la experiencia y se adapte al nuevo contexto.

En la realización de los análisis de riesgos esta proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, por lo cual es la piedra angular, donde se logre controlar cada una de las actividades con fundamento. En la fase de tratamiento es la que se encarga de estructuras cada una de las acciones que se acometen en la seguridad para poder satisfacer cada una de las necesidades que fueron detectadas en el análisis.

Para el Sistema de Gestión de la Seguridad de la Información – SGSI-, la utilización del ciclo PHVA, (Planificar, Hacer, Verificar y Actuar), en esta parte de las diferentes actividades de planificación que se realizan, donde se debe tomar decisiones de tratamiento de los riesgos encontrados, las cuales se plasman en la etapa de implantación, donde se ajusta todos los elementos que admitan la monitorización de las medidas desarrolladas para poder valorar la certeza de las mismas y poder así actuar en consecuencia, dentro de las mejoras continua para la organización.

Ilustración 6. Ciclo PDCA

5.2. Visión de conjunto

Existen dos grandes labores para trabajar:

- Uno es el análisis de riesgos, el cual permite establecer en la Organización y estimar lo que podría pasar a futuro.
- Y como segundo es el tratamiento de los riesgos, el cual permite constituir una defensa minuciosa y prudente, donde se sirva para proteger y al mismo tiempo estar preparados para las emergencias que puedan ocurrir, y así, sobrevivir a los incidentes y seguir trabajando en las condiciones normales; se dice que el riesgo se reduce a un nivel residual que la Dirección de la Organización asume.

El análisis de riesgos se debe considerar los siguientes puntos:

- Los activos son los elementos del sistema de información que soportan la misión para la cual fue creada la Organización.
- Las amenazas son cosas que pueden pasar a los activos causando un perjuicio o deterioro a la Organización.
- Las salvaguardas son las medidas de protección que se despliegan para las amenazas que no causen tanto daño en la Organización.

Es así, que con estos elementos se puede estimar lo siguiente:

- el impacto el cual podría ocasionar

- el riesgo que probablemente pueda pasar

En estos análisis de riesgos permite examinar los elementos anteriores de forma metódica para llegar a las conclusiones con un fundamento y proceder a la fase de tratamiento. La gestión de la seguridad de un sistema de información es la gestión de sus riesgos y del análisis permite coordinar dicha gestión.

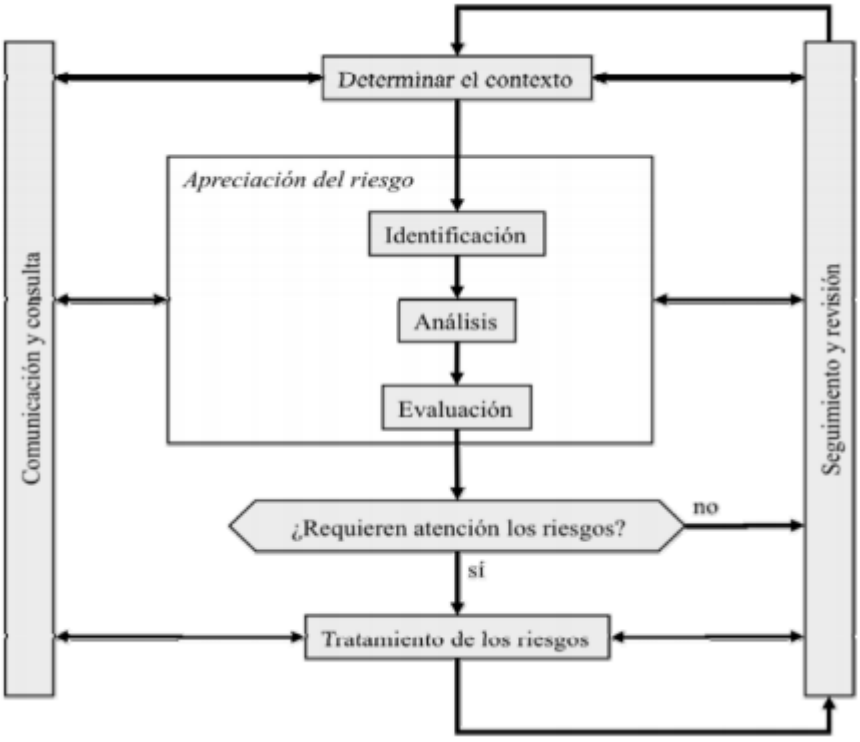


Ilustración 7. Proceso de gestión de riesgos (fuente: ISO 31000).

- La *determinación del contexto* conlleva un valor en los parámetros y condicionantes externos e internos que admiten incluir la política que se realiza para gestionar los riesgos de la organización. Un elemento para recalcar es el alcance de los análisis donde incluye las obligaciones ya sean propias y las contraídas, así como las relaciones con otras organizaciones, donde se desarrolle un intercambio de la información, los servicios y los proveedores de servicios que son contratados.
- La *identificación de los riesgos* de la organización se busca la relación de los potenciales puntos de peligro. Lo que se identifica será analizado en la etapa subsiguiente. Lo que no se logre identificar esto quedará como riesgo oculto o ignorado dentro de la Organización.

- Los *análisis de riesgos* lo que busca calificar los riesgos identificados, realizando un análisis cuantitativo identificando las consecuencias, bien ordenando su importancia relativa.
- La *evaluación de los riesgos* va más allá de un análisis técnico la cual traduce los efectos a términos de la organización. Es aquí donde entran los factores de percepción, estrategia y de las políticas que permitan tomar decisiones respecto a los riesgos que se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.
- El *tratamiento de los riesgos* reúne las diferentes actividades enfocadas a modificar la situación de los riesgos.
- La *comunicación y consulta* son importantes que los sistemas de información deben ser el soporte de la productividad de las Organizaciones.
- En el *Seguimiento y revisión* es importante que en el análisis de los riesgos es una actividad de despacho y es necesario ver qué ocurre en la práctica y así actuar en consecuencia, para así reaccionar oportunamente a cada uno de los incidentes encontrados, para así mejorar continuamente el conocimiento del sistema, con cambio del entorno para mejorar el análisis y ajustarlo.

5.3 Método de análisis de riesgos

El análisis de riesgos es una aproximación metódica para determinar el posible riesgo donde se sigue una serie pasos como son los siguientes:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación cada activo.
2. Determinar a qué amenazas están expuestos los activos.
3. Determinar qué salvaguardas están dispuestos y cuál eficaces son frente a los riesgos.

4. Estimar el impacto definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo definido como el impacto ponderado con la tasa de ocurrencia de la amenaza

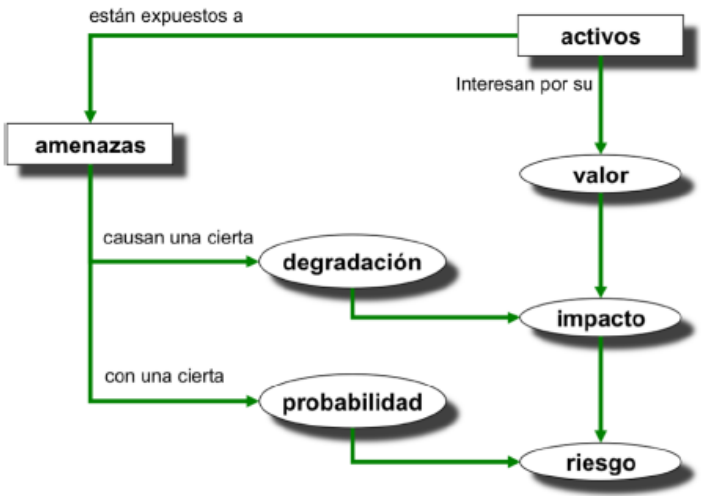


Ilustración 8. Elementos del análisis de riesgos potenciales

Paso 1 - Activos: En un sistema de información hay 2 cosas esenciales, la primera la información que maneja y la segunda los servicios que se presta. No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes (Anexo 1) se encuentra todos los tipos de activos se pueden encontrar en una organización.

De un activo puede interesar calibrar las dimensiones:

- Confidencialidad: Esta valoración es típica de datos, ¿qué daño causaría alguien que conociera lo que no debe?, Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].
- Integridad: Esta valoración es típica de los datos, que pueden estar manipulados, sea total o parcialmente, incluso, faltar datos, ¿qué perjuicio causaría que estuviera dañado o corrupta la información?, Propiedad o característica consistente en que el activo de

información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].

- Disponibilidad: Esta valoración es típica de los servicios, ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?, propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].
- Autenticidad: Los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio, ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?, propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].
- Trazabilidad: Abrir las puertas al fraude, incapacitar a la Organización para perseguir delitos y poder suponer el incumplimiento de obligaciones legales, ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?, Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

SIGLA	SIGNIFICADO
[C]	Confidencialidad
[I]	Integridad
[D]	Disponibilidad
[A]	Autenticidad
[T]	Trazabilidad

Tabla 3. Dimensiones de Valoración

Paso 2 – Amenazas: Consiste en determinar las amenazas que pueden afectar los activos de la organización. Es necesario saber lo que puede pasarle a los activos y el daño que puede causar. Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]. Ver el listado de amenazas en el (anexo 2).

- De origen natural donde hay accidentes naturales.
- Del entorno (de origen industrial) donde hay desastres industriales ante los cuales el sistema de información es víctima pasiva.
- Defectos de las aplicaciones donde hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación.
- Causadas por las personas de forma accidental en el acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- Causadas por las personas de forma deliberada donde las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Valoración de las amenazas

Cuando el activo es una víctima de las diferentes amenazas, no se afecta todas sus dimensiones, ni en la misma cuantía. Una vez determinado cual es la amenaza que puede perjudicar al activo, donde se debe valorar su influencia en el valor del activo, en dos sentidos:

- Degradación: es cuándo lo que perjudica resulta el valor del activo. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones en un activo.

MA	Muy Alta	Casi Seguro	Fácil
A	Alta	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Difícil
MB	Muy Baja	Muy Raro	Extremadamente Difícil

Tabla 4. Degradación del Valor

- Probabilidad: es cuánto existe la probabilidad o improbabilidad es que se materialice alguna amenaza. La probabilidad de ocurrencia es más compleja de determinar y de expresar.

MA	100	Muy Frecuente	A Diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco Frecuente	Cada varios años
MB	1/100	Muy Poco Frecuente	Siglos

Tabla 5. Probabilidad de Ocurrencia

Determinación del impacto potencial

El impacto de acuerdo a la medida del daño en los activos se deriva de la materialización de cualquier amenaza. Conociendo el valor de cada uno de los activos, en las diferentes dimensiones y la degradación que causan las amenazas es directo derivar el impacto que estas generarían sobre el sistema.

- Impacto acumulado

Dicho cálculo sobre un activo teniendo en cuenta, el valor acumulado, el propio más el acumulado de los activos que dependen de él y las amenazas a que está expuesto.

- Impacto repercutido

Dicho calculado sobre un activo teniendo en cuenta, con su valor propio y de las diferentes amenazas a que están expuestos cada uno de los activos.

Determinación del riesgo potencial

El riesgo es la medida del daño probable sobre el sistema de las Organización. Conociendo el impacto de las amenazas sobre cada uno de los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia en cada uno de los activos. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas como se muestra en la siguiente ilustración.

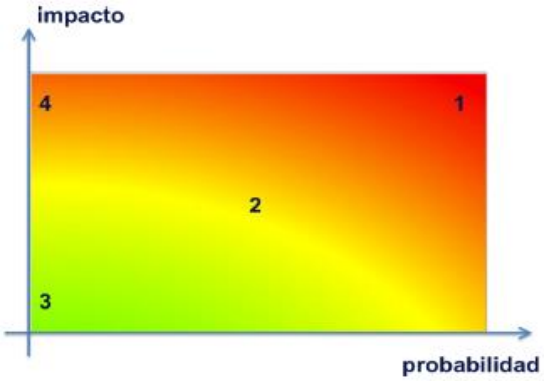


Ilustración 9. El riesgo en función del impacto y la probabilidad.

Zona 1 – Son los riesgos muy probables y de muy alto impacto

Zona 2 – En la franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo

Zona 3 – Son los riesgos improbables y de bajo impacto

Zona 4 – Son los riesgos improbables, pero de muy alto impacto

- Riesgo acumulado es el que se calcula sobre los activos teniendo en cuenta el impacto acumulado sobre los mismos debido a una posible amenaza y la probabilidad de ocurrencia de la misma.
- Riesgo repercutido es el que se calcula sobre un activo teniendo en cuenta el impacto repercutido sobre los mismos debido a una posible amenaza y la probabilidad de la misma.

Paso 3 – Salvaguardas: Se definen las salvaguardas o las contra medidas como aquellos procedimientos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos como son los programas o equipos, otra seguridad física y, por último, está la política del personal. Ver el listado de salvaguardas en el (anexo 3).

Selección de salvaguardas

Ante las múltiples posibles de salvaguardas a considerar, es necesario hacer una selección inicial para quedarse con aquellas que son relevantes para lo que

hay que proteger realmente. En esta selección se debe tener en cuenta los aspectos que me mencionan:

1. Tipo de activos a proteger.
2. Dimensión o dimensiones de seguridad que requieren protección.
3. Amenazas de las que se necesita proteger.
4. Si existen salvaguardas alternativas.

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta los siguientes aspectos:

1. El mayor o menor valor propio o acumulado sobre un activo.
2. La mayor o menor probabilidad de que una amenaza ocurra.
3. La cobertura de riesgo que proporcionan salvaguardas alternativas.

Esto lleva a dos tipos de declaraciones para amparar cierta salvaguarda del conjunto de las que conviene analizarlos así:

- No aplica: Cuando la salvaguarda no es de aplicación porque no es adecuado para el activo a proteger, no protege la dimensión necesaria o no se protege frente a la amenaza en respeto.
- No se justifica: Cuando la salvaguarda aplica, pero es desmedida al riesgo que se tiene que proteger.

Como resultado a lo anterior se dispondrá una “declaración de aplicabilidad” que debe ser analizada como componentes del sistema que está en protección.

Paso 4 - Impacto Residual: Es un conjunto de salvaguardas que se despliegan y una medida de madurez del proceso de gestión, el sistema queda en una situación de posible impacto el cual se denomina residual. La magnitud de la degradación se toma la eficacia de las salvaguardas registrados, la proporción que resta entre la eficacia perfecta y la eficacia real. El impacto residual puede calcularse acumulado sobre los cada uno de los activos inferiores o repercuta sobre los activos superiores.

Paso 5 - Riesgo Residual: Es un conjunto de salvaguardas desplegadas y es una medida en la madurez en los procesos de gestión, el sistema queda en una

situación de riesgo la cual se denomina residual. Se dice que se ha reformado el riesgo, desde el valor potencial a un valor residual, para así se puedan repetir los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación es tomada con respeto en el cálculo del impacto residual y la magnitud de la probabilidad residual es tomada desde la eficacia de las salvaguardas y las proporciona que resta entre la eficacia perfecta y la eficacia real.

El análisis de los riesgos se lleva a cabo siguiendo estas tareas que se continúan:
MAR.1: Caracterización de los activos:

La identificación de los activos más notables dentro del sistema que se va a analizar, donde se caracterizan por tipo de activo, identificando las relaciones que existen entre cada uno de los activos, se debe determinar las dimensiones de seguridad más importantes y valorar la importancia, este resultado de la actividad se denomina el modelo de valor.

Sub-tareas:

- Tarea MAR.11: Identificación de los activos
- Tarea MAR.12: Dependencias entre activos
- Tarea MAR.13: Valoración de los activos

MAR.2: Caracterización de las amenazas

La identificación de las amenazas más importantes sobre el sistema a analizar, donde se caracteriza las estimaciones de ocurrencia de la probabilidad y el daño causado de la degradación, este resultado se denomina “mapa de riesgos”.

Sub-tareas:

- Tarea MAR.21: Identificación de las amenazas
- Tarea MAR.22: Valoración de las amenazas

MAR.3: Caracterización de las salvaguardas

La identificación las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que se pretende atenuar. El resultado de esta actividad se genera en varios informes como son:

- Declaración de aplicabilidad.
- Evaluación de salvaguardas.
- Insuficiencias o vulnerabilidades del sistema de protección.

Sub-tareas:

- Tarea MAR.31: Identificación de las salvaguardas pertinentes
- Tarea MAR.32: Valoración de las salvaguardas

MAR.4: Estimación del estado de riesgo

Esta acción se procesa los datos que fueron recopilados en cada una de las actividades mencionadas anteriormente para realizar un informe del estado de riesgo denominado estimación de impacto y riesgo, otro informe es de insuficiencias, deficiencias o debilidades en el sistema de salvaguardas

Sub-tareas:

- Tarea MAR.41: Estimación del impacto
- Tarea MAR.42: Estimación del riesgo

5.4. Proyectos de análisis de riesgos

Las acciones de los análisis de riesgo son recurrentes en cada proceso de gestión, ya que permanentemente se revisa los análisis y se deben mantener al día. Cuando se realiza por la primera vez el análisis de riesgos y la política de la organización marque que se contemple el manejo de una nueva plataforma. Cuando se elabora un análisis de riesgos iniciando en cero, se consume unos recursos apreciables y conviene planear dichas actividades dentro de un proyecto, el cual puede ser interno o externo.

Las consideraciones que se deben tener en cuenta para que este proyecto llegue a buen término son las siguientes:

PAR.1 – Actividades preliminares

Sub-tareas:

- PAR.11 – Estudio de oportunidad
- PAR.12 – Determinación del alcance del proyecto
- PAR.13 – Planificación del proyecto
- PAR.14 – Lanzamiento del proyecto

PAR.2 – Elaboración del análisis de riesgos

PAR.3 – Comunicación de resultados

5.5 Plan de seguridad

Para llevar a cabo los planes de seguridad, se entiende por proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos encontrados en la organización. Estos planes reciben diferentes nombres de acuerdo con el contextos y circunstancias que se estén desarrollando:

- Plan de mejora de la seguridad.
- Plan director de seguridad.
- Plan estratégico de seguridad.
- Plan de adecuación.

Es así como se identifican las siguientes tareas a trabajar:

PS.1 – Identificación de proyectos de seguridad

PS.2 – Plan de ejecución

PS.3 – Ejecución

5.6 Análisis y tratamiento de los riesgos

Los equipos de desarrollo y los riesgos analizados se trabajan de forma reiterada hasta validar una posible solución que satisfaga cada una de las partes en pro de mejora de la organización. Habitualmente el equipo de desarrollo es el que toma la iniciativa donde propone una posible solución técnica que reconozca los requisitos funcionales del sistema. El análisis del equipo de seguridad validando la propuesta donde se informa los riesgos asociados y se propone las salvaguardas que pudieran dejar los riesgos en niveles aceptables, a esta medida las salvaguardas propuestas afecten el diseño, el equipo genera una modificación a la propuesta inicial, y así, poder realizar un nuevo análisis.

El detalle de las salvaguardas se debe incorporar tanto los mecanismos de actuación como los mecanismos de configuración, monitorización y control de su eficiencia y eficacia en la organización. Es usual que aparezcan algunos desarrollos particularmente destinados a configurar el conjunto de salvaguardas y así poder monitorizar su operación.

Cuando los dos equipos lleguen a una situación estable, con un diseño técnicamente factible, con un riesgo y unos requisitos aceptables de recursos, la propuesta se eleva al comité para su debida aprobación. Como resultado de esta fase, se dispone las especificaciones técnicas de desarrollo las cuales van acompañadas de un análisis de los riesgos y sus decisiones de tratamiento.

6. VULNERABILIDADES DE UN SISTEMA

Las vulnerabilidades son las debilidades que ponen en peligro toda una red y por ende existen los expertos en ciberseguridad para aliviar las amenazas y sus correspondientes tipos de vulnerabilidades. Existen dos tipos de vulnerabilidades en las cuales son las siguientes:

- Las físicas
- Las lógicas

Vulnerabilidades lógicas

Son las afectan directamente la infraestructura y el desarrollo de la operación de estos las cuales pueden ser las siguientes:

- La configuración en el sistema operativo por los defectos o incluso de algunas aplicaciones en el servidor el cual este expuesto, adicional también se debe tener en cuenta la configuración de los firewalls que no estén funcionando de manera correcta
- La actualización en las organizaciones las cuales no se realicen estas pueden estar expuestas a las nuevas vulnerabilidades y estas se deben tener en cuenta a futuro.
- En el desarrollo son aquellas que generan los ataques por medio de las inyecciones de código en SQL, Cross Site Scripting, las cuales puede variar dependiendo del tipo de aplicación y la validación de los datos.

Existen dos maneras para descubrir las vulnerabilidades existentes:

1. A través de búsquedas por parte de ciberdelincuentes que intentan sacar el máximo beneficio hasta que la vulnerabilidad se haga pública y se desarrolle los parches pertinentes por parte de los programadores de cada aplicación.
2. A través de las publicaciones en grupos de hacktivistas como The Shadow Brokers y otros grupos que existen para contener los ataques cibernéticos.

En los sistemas informáticos de una organización lo que se debe proteger son los activos de la empresa como son los recursos que forman parte del sistema y se agrupan de la siguiente manera:

- Hardware: comprende los elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento.
- Software: comprende el conjunto de programas que se ejecutan sobre el hardware, sean del propio sistema operativo como las aplicaciones instaladas en él.
- Datos: comprenden la información lógica que es procesa por el software haciendo uso del hardware. En general es la información estructurada en bases de datos o paquetes de información que viajan por la red.
- Otros: son aquellos que se usan y gastan en los diferentes periféricos del hardware, pero al ser elementos externos al sistema informático no son críticos para su seguridad.

De los grupos anteriormente mencionados uno de los más críticos son los datos, el hardware y el software. Es así, los datos son almacenados en el hardware y son procesados por las diferentes aplicaciones denominadas software.

El activo más delicado son los datos. El resto se puede restablecer con facilidad y los datos depende de que la empresa tenga una política de copias de seguridad y sea capaz de restablecer en el estado más próximo al momento en que se realizó la pérdida. Esto conllevaría a una organización la dificultad de reponer dicha información con lo que acarrearía pérdida de tiempo y de dinero.

Las vulnerabilidades de los sistemas informáticos se agrupar en función de su:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.

- Políticas de seguridad deficientes e inexistentes.

Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Configuración inadecuada de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

6.1 Vulnerabilidad del día cero

- Cuando no exista una solución “conocida” para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como “vulnerabilidad 0 days”.

Globalmente las vulnerabilidades se clasifican de la siguiente manera:

- Desbordamiento de buffer, esta se produce cuando un programa no controla la cantidad de datos que se copian en el buffer, de forma que si esa cantidad es superior a la capacidad del buffer de los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original.
- Condición de carrera o race condition, se da principalmente cuando varios procesos acceden al mismo tiempo a un recurso compartido, como una variable, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma.
- Error de formato de cadena o format string bugs, la causa principal es aceptar sin validar la entrada de datos proporcionada por los usuarios. Es un error de programación y el lenguaje que afecta es C/C++. Un ataque

puede conducir de manera inmediata a la ejecución de código arbitrario y a revelación de información confidencial por la organización.

- Cross Site Scripting o XSS, abarcaba cualquier ataque que permitiera ejecutar scripts como VBScript o JavaScript, en el contexto de otro sitio web. Estos errores se pueden encontrar en cualquier aplicación que tenga como objetivo final presentar la información en un navegador web.
- Inyección SQL, se produce cuando se inserta un código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código invasor en la base de datos.
- Denegación del servicio, se provoca cuando un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red en la organización por el consumo excesivo del ancho de banda de la red o el consumo de los recursos informáticos del sistema de la víctima.
- Ventanas engañosas o Window Spoofing, son aquellas que dicen que eres el ganador de un premio, lo cual es mentira y lo único que quieren es que proporcione información. Existe otro tipo de ventanas que, si se le da clic, logra obtener los datos del ordenador para posteriormente realizar un ataque ya sea al equipo o a la organización.

En la detección de vulnerabilidades en las redes de datos una del software a utilizar es Kali-Linux este permite la utilización herramientas como las siguientes:

- Traceroute: Diagnóstica la red donde es capaz de mostrar la ruta completa de una conexión, así como medir los retrasos de tránsito de los paquetes enviados a través de una red IP.
- WhatWeb: Identifica los sitios web, incluyendo CMS’s como wordpress, otras plataformas de blogging, paquetes estadísticos y/o analíticos, bibliotecas de Javascript, servidores web y dispositivos integrados. Whatweb además más de 1700 plugins, con diferentes funcionalidades. Adicional identifica número de versión, direcciones de correo electrónico, errores de SQL y muchas más.

- Nmap: Es utilizada para la detección de redes y las auditorias de seguridad. Una de las opciones más potentes de las muchas que tiene, es el modificador del "*script vuln*" que hace que NMap escanee y audite la seguridad de todos los puertos abiertos con la herramienta NSE.
- Nikto: Es un servidor web y una herramienta de evaluación de aplicaciones web para encontrar posibles problemas de seguridad y vulnerabilidades, esta escanea para detectar hasta 6700 potenciales archivos o programas peligrosos.
- SQLiv: Es un escáner de vulnerabilidades de inyección SQL simple y masivo.
- BurpSuite: Es una colección de diferentes herramientas integradas en una única suite que te permite realizar pruebas de seguridad en las aplicaciones web, desde el mapeo inicial y el análisis de la superficie hasta la búsqueda y explotación de vulnerabilidades de seguridad.
- Wireshark: Se encarga de analizar los paquetes de la red, los cuales luego se puede abrir y ver de manera detallada lo que significa.
- Suite aircrack-ng: Permite comprobar la robustez de la clave Wi-Fi, ya que permite auto atacarte tanto por fuerza bruta como por ataque de diccionario para las WPA. Esta suite, vienen programas como el airmonng, el aireplay, airodump o aircrack, los cuales están relacionados entre sí y trabajan juntos por romper las contraseñas de los WIFI.
- Nessus: Es un escaneo de los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en Nessus Attack Scripting Language, un lenguaje scripting optimizado para interacciones personalizadas en redes.

De las anteriormente mencionadas herramientas estas se clasifican en grupos como es la recopilación de información, Análisis de vulnerabilidad, herramientas de explotación, ataques inalámbricos, herramientas forenses, aplicaciones web, pruebas de estrés, oler y suplantar, ataques de contraseña, mantener el acceso, ingeniería inversa, piratería de hardware y herramientas

de informes. Cada uno de estos grupos manejan un determinado de herramientas que validan las vulnerabilidades de la red, realizar un descifrado de las contraseñas por medio de los ataques, sin olvidar que se puede ingresar a las bases de datos por un ataque SQL.

La diferencia entre una vulnerabilidad y un riesgo, donde los riesgos de seguridad cibernética se clasifican comúnmente como vulnerabilidades. Sin embargo, la vulnerabilidad y el riesgo no son lo mismo, lo que puede generar confusión. Piense en el riesgo como la probabilidad y el impacto de una vulnerabilidad que se explota.

Si el impacto y la probabilidad de que una vulnerabilidad sea explotada es baja, entonces el riesgo es bajo. Inversamente, si el impacto y la probabilidad de que una vulnerabilidad sea explotada es alta, entonces existe un alto riesgo.

6.2 Vulnerabilidades de las Bases de Datos

La mayoría de información que se maneja en el mundo es almacenada en diferentes gestores de bases de datos como lo son Oracle, MySQL, Microsoft SQL Server y otros que son usados dependiendo del sistema operativo. Esta información para los hackers es de vital importancia y es así que centren todo el esfuerzo para poder acceder y conseguir dicha información por lo cual se explora las diferentes vulnerabilidades en las organizaciones.

A continuación, se relacionan algunas de las vulnerabilidades que son más expuestas las organizaciones:

6.2.1 Características de bases de datos innecesariamente habilitadas

Una instalación nueva de una base de datos en las organizaciones estas vienen con una serie de módulos adicionales de distintas formas y tamaños que en pocas ocasiones todos ellos son utilizadas por las organizaciones, lo que convierte en una puerta de entrada en la cual se puede sufrir un ataque por cualquiera de los paquetes que generan un problema de seguridad.

6.2.2 Preferencia de privilegios de usuario por privilegios de grupo

En ocasiones muchos usuarios reciben más privilegios sobre la base de datos de los que realmente necesitan, lo que a la larga se puede convertir en un importante problema. Es recomendable modificar los privilegios otorgados a los usuarios que estarán en contacto con la información con el fin de que no puedan realizar modificaciones más allá de las autorizadas[39].

6.2.3 Desbordamiento de búfer

Se trata de otro de los medios favoritos utilizados por los piratas y que se dan por el exceso de información que se puede llegar a enviar por medio del ingreso de información mediante el uso de formularios, es decir, se recibe mucha más información de lo que la aplicación espera. Por poner un ejemplo, si se espera la entrada de una cuenta bancaria que puede ocupar unos 25 caracteres y se permite la entrada de muchos más caracteres desde ese campo, se podría dar este problema[40].

6.2.4 Nombre de usuario/password en blanco o bien hacer uso de uno débil

Hoy en día no es raro encontrarnos pares de datos usuario/password del tipo admin/12345 o similar. Esta es la primera línea de defensa de entrada a nuestra información y debemos optar por el uso de algo más complejo que sea complicado de conseguir por parte de cualquier atacante[41].

6.2.5 Datos sensibles sin cifrar

Aunque pueda ser algo obvio, a la hora de la verdad no todo el mundo cifra la información más importante que se almacena en base de datos. Esto es una buena práctica para que en caso de hackeo, sea complicado para el atacante poder recuperar esa información[42].

---

[39] Telefónica. Bases de datos y sus vulnerabilidades más comunes. p 3
[40] Ibid., p 3
[41] Ibid.., p 2
[42] Ibid.., p 4

6.2.6 Bases de datos sin actualizar

Como ocurre con cualquier tipo de aplicación que tengamos instalada en nuestra máquina, es necesario ir actualizando la versión de nuestra base de datos con las últimas versiones lanzadas al mercado, ya que en ellas se solucionan aquellos problemas de seguridad detectados, por lo que pondremos más barreras a los posibles atacantes[43].

6.3 Vulnerabilidades de las Páginas WEB

Las vulnerabilidades en las aplicaciones en las páginas WEB son para poder desplegar el código de la misma. La plataforma sobre la que se despliega la aplicación esté correctamente reforzada para poder evitar las vulnerabilidades que se mencionan a continuación y así evitar el riesgo de que puedan ser atacadas.

6.3.1 Injection

Las fallas de inyección, como la inyección de SQL, NoSQL, OS y LDAP, ocurren cuando se envían datos que no son de confianza a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a los datos sin la debida autorización[44].

6.3.2 Broken Authentication

Las funciones de la aplicación relacionadas con la autenticación y la administración de sesiones a menudo se implementan de manera incorrecta, lo que permite a los atacantes comprometer contraseñas, claves o tokens de sesión, o aprovechar otras fallas de implementación para asumir las identidades de otros usuarios de forma temporal o permanente[45].

---

[43] Ibid.., p 4
[44] OWASP. OWASP Top Ten.
[45] Ibid..

6.3.3 Sensitive Data Exposure

Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales, como los financieros, la atención médica y la PII. Los atacantes pueden robar o modificar esos datos débilmente protegidos para cometer fraude con tarjetas de crédito, robo de identidad u otros delitos. Los datos confidenciales pueden verse comprometidos sin protección adicional, como el cifrado en reposo o en tránsito, y requieren precauciones especiales cuando se intercambian con el navegador[46].

6.3.4 XML External Entities (XXE)

Muchos procesadores XML más antiguos o mal configurados evalúan las referencias de entidades externas dentro de los documentos XML. Las entidades externas se pueden utilizar para divulgar archivos internos mediante el controlador de archivos URI, recursos compartidos de archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio[47].

6.3.5 Broken Access Control

Las restricciones sobre lo que pueden hacer los usuarios autenticados a menudo no se aplican correctamente. Los atacantes pueden aprovechar estas fallas para acceder a funciones y / o datos no autorizados, como acceder a las cuentas de otros usuarios, ver archivos confidenciales, modificar los datos de otros usuarios, cambiar los derechos de acceso, etc[48].

6.3.6 Security Misconfiguration

La mala configuración de seguridad es el problema más común. Esto suele ser el resultado de configuraciones predeterminadas inseguras, configuraciones incompletas o ad hoc, almacenamiento en la nube abierta, encabezados HTTP mal configurados y mensajes de error detallados que contienen información confidencial. No solo todos los sistemas operativos, marcos, bibliotecas y

[46] Ibid…
[47] Ibid….
[48] Ibid….

aplicaciones deben estar configurados de manera segura, sino que también deben ser parcheados / actualizados de manera oportuna[49].

6.3.7 Cross-Site Scripting (XSS)

Los defectos de XSS ocurren cuando una aplicación incluye datos que no son de confianza en una nueva página web sin la validación o el escape adecuados, o actualiza una página web existente con datos proporcionados por el usuario mediante una API de navegador que puede crear HTML o JavaScript. XSS permite a los atacantes ejecutar scripts en el navegador de la víctima que pueden secuestrar sesiones de usuario, desfigurar sitios web o redirigir al usuario a sitios maliciosos[50].

6.3.8 Insecure Deserialization

La deserialización insegura a menudo conduce a la ejecución remota de código. Incluso si las fallas de deserialización no dan como resultado la ejecución remota de código, se pueden usar para realizar ataques, incluidos ataques de reproducción, ataques de inyección y ataques de escalada de privilegios[51].

6.3.9 Using Components with Known Vulnerabilities

Los componentes, como bibliotecas, marcos y otros módulos de software, se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, dicho ataque puede facilitar la pérdida de datos o la toma de control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden socavar las defensas de las aplicaciones y permitir varios ataques e impactos[52].

6.3.10 Insufficient Logging & Monitoring

El registro y la supervisión insuficientes, junto con una integración faltante o ineficaz con la respuesta a incidentes, permiten a los atacantes atacar aún más los sistemas, mantener la persistencia, cambiar a más sistemas y manipular,

[49] Ibid….
[50] Ibid…..
[51] Ibid…..
[52] Ibid…..

extraer o destruir datos. La mayoría de los estudios de infracciones muestran que el tiempo para detectar una infracción es de más de 200 días, generalmente detectados por partes externas en lugar de procesos internos o monitoreo[53].

6.4 Vulnerabilidades en las Redes

Las vulnerabilidades en las redes son de un grado de debilidad inherente al diseño de la red de la organización y de los dispositivos que son utilizados, donde esto incluye los routers, computadoras de escritorio, switches, servidores y dispositivos de seguridad.

6.4.1 Portátiles y Netbooks

Las compañías tienen información sensible que no debe salir de sus oficinas. Esto se convierte en un peligro cuando la información está almacenada en un portátil no seguro. A menos que el portátil utilice un algoritmo de encriptación, los datos pueden ser recuperados por cualquiera[54].

6.4.2 Variedad de dispositivos USB

Si un end point puede leer y ejecutar datos desde un dispositivo, puede presentar tanto peligro como un pendrive. Tal es el caso de cámaras digitales, reproductores de MP3 e incluso marcos digitales. En 2008, Best Buy declaró que habían encontrado un virus en los marcos de fotos Insignia que procedían directamente del fabricante[55].

6.4.3 Los lectores USB

La ubiquidad de estos lectores ha llevado a los hackers a desarrollar malware específico como el conocido gusano Conficker, que se ejecuta de forma automática al conectar la llave al USB. Este problema se intensifica con las

[53] Ibid…..
[54] Universidad Libre. Top 10 de las vulnerabilidades internas de las redes: ¡El peligro está dentro! 2015.
[55] Ibid.., 2015

configuraciones por defecto de muchos sistemas operativos que ejecutan automáticamente la mayoría de los programas (incluyendo los maliciosos)[56].

6.4.4 Medios ópticos

Al igual que con los dispositivos USB que mencionábamos antes, es importante implementar y reforzar el control y las políticas de acceso respecto a los dispositivos que pueden acceder a la red como los CDs[57].

6.4.5 Smartphones y otros dispositivos digitales

Estos nuevos dispositivos presentan las mismas amenazas que los portátiles y las llaves USB. La importancia de estos dispositivos radica en su potencialidad para eludir las soluciones DLP tradicionales. Aplique las mismas reglas que a los dispositivos USB y medios ópticos[58].

6.4.6 Puntos de Acceso inalámbrico (APs)

Los ataques a redes inalámbricas realizados por Wardrivers son comunes y han causado graves daños. Por ejemplo, TJ Stores, propietario de Marshalls y TJMaxx, sufrió un ataque a través de este método; los intrusos penetraron en los ordenadores de su oficina en los que se guardaba datos de transacciones de sus clientes como la tarjeta de crédito, de debido y cheques. Este ataque supuso para la compañía un coste de más de 500 millones de dólares. El protocolo de encriptación inalámbrica (WEP) contiene conocidas vulnerabilidades que se ven afectadas por ataques como Aircrack[59].

6.4.7 Conexiones internas

Los empleados de una compañía pueden acceder, accidental o premeditadamente, a áreas de la red corporativa a las que no deberían tener acceso. Se deben cambiar las claves regularmente y cumplir con las políticas de autenticación y acceso[60].

---

[56] Ibid..., 2015
[57] Ibid..., 2015
[58] Ibid...., 2015
[59] Ibid....., 2015
[60] Ibid....., 2015

6.4.8 El troyano humano

El troyano humano se adentra en la empresa camuflado, de hombre de negocios, con un mono de operario y en menos de un minuto puede infectar la red corporativa desde la sala de servidores. Hay que recordar a los empleados que deben pedir las autorizaciones a personas ajenas a la organización identificándoles[61].

6.4.9 Email

Los emails pueden ser en sí mismos un foco de infección. Un correo electrónico es capaz de sustraer las credenciales de acceso de un empleado. Este robo puede ser utilizado para futuros ataques. En el caso de la seguridad del correo electrónico, identificar la fuente es clave. Podemos conocer quién es el emisor utilizando tecnología PGP o con unas cuantas preguntas antes de enviarle información sensible[62].

6.5 Motores de búsqueda de vulnerabilidades

La agencia National Vulnerability Database del gobierno de EE.UU. donde utilizan los datos de gestión de vulnerabilidades la cual se basa en estándares representados mediante los Protocolos de automatización de contenido de seguridad (SCAP). Los datos permiten la automatización de la gestión de vulnerabilidades, la medición de seguridad y el cumplimiento. El NVD incluye en sus bases de datos de referencias las listas de verificación de seguridad, fallas de software relacionadas con la seguridad, configuraciones incorrectas, nombres de productos y métricas de impacto.

Originalmente creado en el año 2000 donde se llamó Internet - Categorization of Attacks Toolkit o ICAT, el NVD ha experimentado múltiples iteraciones y mejoras, las cuales permiten continuar mejorando cada uno de los servicios que se

[61] Ibid....., 2015
[62] Ibid....., 2015

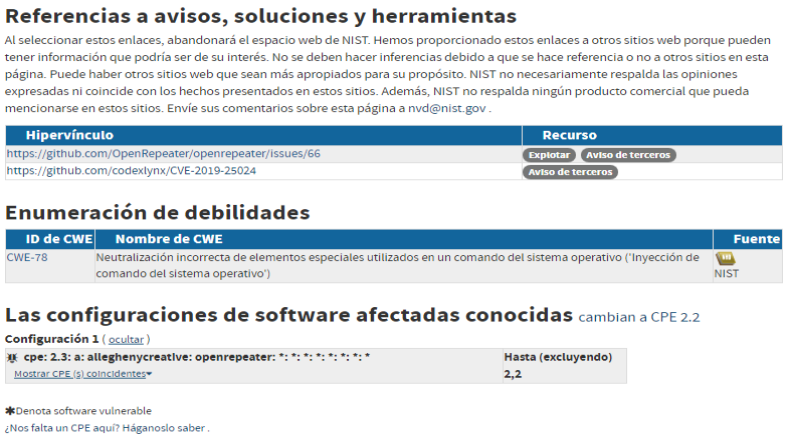
ofrecen. El NVD es un producto de la División de Seguridad Informática del NIST, el laboratorio de Tecnología de la Información el cual está patrocinado por la Agencia de Seguridad de Infraestructura y Ciberseguridad.

Dicha agencia realiza un análisis de los CVE que se han publicado en el Diccionario CVE. El personal de NVD tiene la tarea de analizar los CVE mediante la agregación de puntos de datos de la descripción, las referencias proporcionadas y cualquier dato complementario que se pueda encontrar públicamente. Este análisis da como resultado métricas de impacto de asociación (Common Vulnerability Scoring System - CVSS), tipos de vulnerabilidad (Common Weakness Enumeration - CWE) y declaraciones de aplicabilidad (Common Platform Enumeration - CPE), así como otros metadatos pertinentes. El NVD no realiza pruebas de vulnerabilidad de forma activa, confía en cada uno de los proveedores, investigadores de seguridad de terceros y coordinadores de vulnerabilidades que proporcionar información, esta información se utiliza para asignar cada uno de los atributos. A medida que se disponga de información adicional, los puntajes CVSS, los CWE y las declaraciones de aplicabilidad están sujetos a cambios.

En el siguiente enlace https://nvd.nist.gov/search, se puede realizar la consulta de los cada uno de los CVE que han sido registrados, donde se puede validar la vulnerabilidad y el nivel de afectación que tiene el mismo.

Ilustración 10. Ejemplo de CVE

En el anterior ejemplo se puede visualizar el número de la publicación y en el año que fue expuesto, adicional informa la descripción de la vulnerabilidad y el análisis que presenta la misma, aparte de esto presenta el nivel de afectación en cada uno de los niveles, asi, bajo, medio, crítico y alto.



Referencias a avisos, soluciones y herramientas

Al seleccionar estos enlaces, abandonará el espacio web de NIST. Hemos proporcionado estos enlaces a otros sitios web porque pueden tener información que podría ser de su interés. No se deben hacer inferencias debido a que se hace referencia o no a otros sitios en esta página. Puede haber otros sitios web que sean más apropiados para su propósito. NIST no necesariamente respalda las opiniones expresadas ni coincide con los hechos presentados en estos sitios. Además, NIST no respalda ningún producto comercial que pueda mencionarse en estos sitios. Envíe sus comentarios sobre esta página a nvd@nist.gov .

Hipervínculo	Recurso
https://github.com/OpenRepeater/openrepeater/issues/66	Explotar Aviso de terceros
https://github.com/codexlynx/CVE-2019-25024	Aviso de terceros

Enumeración de debilidades

ID de CWE	Nombre de CWE	Fuente
CWE-78	Neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo ('Inyección de comando del sistema operativo')	NIST

Las configuraciones de software afectadas conocidas cambian a CPE 2.2

Configuración 1 (ocultar)

cpe: 2.3: a: alleghenycreative: openrepeater: *: *: *: *: *: *: *: *	Hasta (excluyendo)
Mostrar CPE (s) coincidentes	2,2

*Denota software vulnerable

¿Nos falta un CPE aquí? Háganoslo saber .

Ilustración 11. Ejemplo de CVE 2

Además, existen un sin número de herramientas para escanear las vulnerabilidades donde las organizaciones se pueden apoyar para realizar los análisis automatizados de cualquier aplicación, sistema o red en busca de cualquier posible vulnerabilidad que exista. Aunque estas aplicaciones no son capaces de detectar la vulnerabilidad con total precisión, sí son capaces de detectar ciertos elementos que podrían desencadenar en una vulnerabilidad, lo que facilita enormemente el trabajo de los investigadores o ingenieros. Existen varios tipos de escáneres de vulnerabilidades:

- Autenticados, son los que permiten realizar pruebas y ataques potenciales desde la propia red.
- No autenticados, son donde el investigador o hacker ético se intenta hacer pasar por un pirata informático simulando un ataque desde fuera para ver hasta dónde es capaz de llegar analizando las posibles vulnerabilidades.

Las siguientes son algunas herramientas que pueden ser utilizadas para validar las vulnerabilidades de la red de las organizaciones:

- **Nmap:** Es un software el cual ayuda a buscar hosts dentro de una red local, pero también permite el descubrimiento de hosts en Internet para comprobar si están conectados a la red, además, permite realizar amplios y avanzados escaneos de puertos para comprobar si existe algún servicio funcionando que no esté protegido por el firewall, e incluso poder ver si existe un firewall en un determinado host.

- **Aircrack-ng:** esta herramienta permite poner a prueba la seguridad de cualquier red Wi-Fi en busca de una posible vulnerabilidad que permita a cualquier usuario no autorizado hacerse de la contraseña de la red. Este programa es uno de los más utilizados en el mundo para crackear redes WiFi, ya sea con cifrado WEP, WPA e incluso WPA2, no obstante, normalmente se utiliza junto con otros programas para acelerar la tarea de crackeo de las contraseñas.
- **Hashcat**: esta herramienta sirve para crackear todo tipo de hashes de las contraseñas, es un programa para realizar ataques de diccionario o fuerza bruta contra el hash de una clave para intentar crackearla. Hashcat utiliza la potencia de la CPU y GPU para acelerar lo máximo posible el proceso de obtención de la clave.
- **Wireshark:** es un analizador de cada uno de los paquetes y protocolos que pasan por la red, esta aplicación es capaz de registrar absolutamente todos los paquetes que pasan por la red de las organizaciones, recogerlos, poder filtrar y ordenar de multitud e formas para poder analizar cómodamente todo el tráfico. Esta herramienta además es capaz de descifrar los paquetes enviados a través de los principales protocolos de conexión segura para poder analizar sin problema su contenido.
- **OpenVAS**: es un escáner de vulnerabilidades en el que se puede introducir una dirección IP y encargarle el análisis de dicho equipo, recogiendo información sobre los servicios en funcionamiento, los puertos abiertos, fallos de configuración, posibles vulnerabilidades conocidas en el software de cada uno de los equipos o servidores.

Estas son algunas herramientas que les sirven a las organizaciones para poder validar las vulnerabilidades que existen internamente de la red, para lograr generar los diferentes planes de acción y las alternativas para poder evitar un ciberataque por los diferentes grupos que existen no solo en Colombia sino en el mundo.

7. COMPARACIONES DE METODOLOGIAS

En la actualidad para realizar los diferentes análisis de riesgos dependiendo de las PyMES, se pueden utilizar las siguientes de acuerdo con lo que disponga los recursos de cada una de las organizaciones

7.1 Metodología Octave

Ámbito de Aplicación

Pymes, Organizaciones públicas y privadas

Ventajas

- Es autodirigidle. Se puede desarrollar por los empleados de la organización, utilizando un equipo multidisciplianrio.
- Involucra a todo el personal.
- Construye los perfiles de amenazas basados en los activos.
- Identifica la vulnerabilidad de la infraestructura.
- Desarrolla planes y estrategias de seguridad.
- Comprende etapas de análisis y gestión de los riesgos.
- Involucra proceso, dependencias, vulnerabilidades, activos, recursos salvaguardas y amenazas.
- Relaciona las amenazas y vulnerabilidades
- El uso es interno y gratuito.
- Posee tres métodos Octove, Octave-s y Octave allegro que son adaptables a la organización.

Desventajas

- No tiene en cuenta el principio de no repudio de la información
- Utiliza demasiados documentos para el proceso de análisis de riesgos.
- Se requiere de conocimientos técnicos muy amplios.
- No se define claramente los diferentes activos de la información.

- El uso externo, se debe comprar la licencia SEI si se requiere implementar la metodología por un tercero.

7.2. Metodología MAGERIT

Ámbito de Aplicación

Gobierno, Compañías Grandes Comerciales y No comerciales, PyMES

Ventajas

- Alcance completo en el análisis y gestión de los riesgos.
- Está muy bien documentada en cuanto los recursos de información, amenazas y tipos de activos.
- Utiliza un complejo análisis de riesgos cuantitativos y cualitativos.
- Es de libre y no requiere ninguna autorización.
- Divide los activos de la organización en grupos, para lograr identificar más los riesgos y así poder tomar las contramedidas para evitar cualquier riesgo.
- Se centra en 3 objetivos, concientizar sobre la existencia de los riesgos y la necesidad de contenerlos a tiempo, ofrece un método sistemático para analizar los riesgos para ayudar a descubrir y planificar las medidas oportunas para manejar los riesgos bajo control.
- Prepara a la organización en los procesos de evaluación, auditoria, certificación o acreditación de la norma.
- Permite que el proceso esté bajo supervisión y control en cualquier momento y contempla aspectos prácticos para la realización de los análisis y una gestión de riesgos efectiva.
- Tiene una buena base documental los cuales están en 3 libros, El método, Catalogo de elementos y guía de técnicas. Esta información es de acceso público.
- Maneja la herramienta para el análisis de riesgos como PILAR.

Desventajas

- Es un modelo que no involucra los procesos, recursos ni las vulnerabilidades.
- Posee falencias en el inventario de políticas.
- Se considera una metodología costosa en su aplicación.

7.3. Metodología MEHARI

Ámbito de Aplicación

Gobierno, Empresas grandes y mediadas, Compañías comerciales sin ánimo de lucro.

Ventajas

- Para el análisis de riesgos utiliza un modelo tanto cuantitativo como cualitativo.
- Es un método capaz de evaluar y lograr la disminución de los riesgos en función del tipo de organización.
- Contiene unas bases de datos de conocimientos los cuales tienen manuales, guías y herramientas que permiten realizar el análisis de riesgo cuando se requiera.
- Complementa y se acopla a las necesidades de las normas ISO 27001, 27002 y 27005 para poder definir el SGSI y la gestión del riesgo.
- Por medio de esta metodología se detectan vulnerabilidades mediante auditorias y se analizan las diferentes situaciones de riesgo.
- Combina el análisis y la evaluación de riesgos; específicamente el módulo de evaluación rápido y otra de evaluación detallada.

Desventajas

- Se enfoca solo en los principios de la integridad, confiabilidad y disponibilidad, por lo cual olvida el repudio.

- La recomendación de los controles no se incluye dentro del análisis sino dentro de la gestión del riesgo.
- El impacto de los riesgos se estima en el proceso de gestión y evaluación.

7.4. Metodología EBIOS

Ámbito de Aplicación

Sector público, Pequeñas y grandes empresas

Ventajas

- Ayuda a las organizaciones a tener un mayor reconocimiento en las diferentes actividades de seguridad ya que tiene compatibilidad con las normas internacionales ISO.
- Es una herramienta de negociación y de arbitraje.
- Se utiliza para múltiples finalidades y procedimientos de seguridad en las organizaciones.
- Es una herramienta de código libre y reutilizable.
- Se ajusta al cumplimiento de las normas ISO 27001, 27005 y 31000.
- Es una herramienta de concienciación para involucrar a cada una de las partes de la organización.
- Contiene una base de conocimiento que describe los tipos de entidades, métodos de ataque, vulnerabilidades, objetivos y los requerimientos de seguridad.

Desventajas

- Se constituye más como una herramienta de soporte que como una metodología.

7.5. Metodología CORAS

Ventajas

- Posee diferentes herramientas que apoyan el análisis de riesgo, un editor gráfico para poder soportar la elaboración de modelos basados en Microsoft Visio y utiliza el lenguaje UML.
- Contiene un repositorio de paquetes de experiencia reutilizables.
- Provee un reporte de las vulnerabilidades que se encuentran.
- Es útil para el desarrollo y mantenimiento del sistema.
- Se basa en modelos de riesgo de sistemas de seguridad críticos.

Desventajas

- No realiza análisis de riesgo cuantitativo.
- Su modelo no tiene contémplanos los elementos como los procesos y/o las dependencias.

7.6. Metodología NIST SP 800 - 30

Ámbito de Aplicación

Organizaciones Gubernamentales y no Gubernamentales.

Ventajas

- Bajo costo relacionado con el riesgo abalizado y solventado.
- Proporciona una guía para la evaluación de los riesgos de seguridad de las infraestructuras de las TI.
- Presenta un resumen de los elementos que son importantes en las pruebas de seguridad técnica y la evaluación con énfasis en técnicas específicas, sus beneficios, limitaciones y recomendaciones para su utilización.
- La guía contiene las herramientas para la valoración y mitigación de riesgos.

- Asegura que los sistemas informáticos que almacena procesan y trasmitan la información.
- Mejora la administración que a partir de los resultados del análisis de riesgo.
- Aplica el análisis y la gestión de los riesgos.

Desventajas

- Es un modelo que no tiene contemplados elementos como son los procesos, los activos y tampoco las dependencias.

8. ESTRATEGIA PROTECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

En la protección de seguridad de la información de las PyMES en la actualidad es de vital importancia, un ataque cibernético puede afectar de manera significativa la infraestructura de la organización donde el riesgo económico y social se ve comprometido hasta el punto de que se cierre la organización por tal ataque.

Por lo anterior, para minimizar el impacto de los ataques y riesgos a los cuales están expuestos las organizaciones se deben realizar y garantizar las siguientes prácticas en la protección de la información.

8.1. Gestión y control de antivirus y antispam.

Se debe validar cada uno de los equipos de la organización para que cuenten con el sistema de gestión del antivirus corporativo, el cual realice análisis periódicos en los equipos donde evite posibles infecciones.

En la actualidad existe una gran variedad de herramientas que facilita la ejecución donde también se tiene en cuenta el mantenimiento adecuado. Es muy importante tener una programación periódica donde se valida que se encuentre actualizado y adicional que se estén ejecutando cada uno de los protocolos que se establecen al momento de configurarlo.

Es muy importante también tener instalado los antispam el cual permite evitar malware que puede borrar o dañar archivos, phishing o robo de claves de acceso y demás otras funciones muy importantes.

8.2. Gestión de Actualizaciones Automáticas.

Se debe revisar las actualizaciones de las bases de datos de los servidores, parches de seguridad, vulnerabilidades y demás, si se realizan correctamente. Es de vital importancia no dejar de revisar que las actualizaciones se realicen correctamente. Para la organización debe tener una buena distribución y

configuración, donde facilite la gestión, pero lo más importante es que se debe revisar que todo se realice correctamente.

Las nuevas vulnerabilidades se descubren cada semana las cuales afectan a los sistemas operativos, los navegadores incluso los mismos antivirus. Detrás de cada programa existen grandes equipos de ingenieros que solventan cada uno de los problemas y brechas de seguridad las cuales se mejoran con las nuevas versiones, es así, que una buena revisión periódica evita muchos problemas en las organizaciones.

8.3. Gestión de Copias de Seguridad.

Generar las copias de seguridad fiables de toda la información relevante en la organización, dicha información no sólo puede estar amenazada por robos o programa maligno, también por diferentes sucesos que puedan ocurrir como son las inundaciones o incendios o cualquier catástrofe natural. Estas copias de seguridad se deben hacer en dispositivos externos, desde discos duros hasta servidores dedicados.

Plantear una buena estrategia de copias de seguridad con los equipos informáticos los cuales pueden sufrir fallos, borrados o perdidas de información accidental o deliberada. Por ello, se la política de copias de seguridad de toda la información que considere importante para la organización. Para así cuando se restablezca el servicio se ponen a funcionar las copias de seguridad y así la organización inicia sus labores sin mayores sobre saltos.

8.4. Gestión de incidentes de seguridad.

Gestionar los incidentes de seguridad correctamente los que surgen en la organización es de vital importancia. Primero se identifica el incidente el cual puede ser recepcionado por notificación de un usuario o por identificación desde el departamento de tecnología mediante el análisis de logs o anomalías en los sistemas. Posteriormente se debe clasificar en la base de acuerdo con su criticidad, tipología, equipos afectados y demás para finalmente mitigarlo y

contenerlo. Y finalmente se debe recuperar los sistemas afectados y documentar cada paso de lo ocurrió.

8.5. Gestión de la Monitorización.

Las organizaciones es imprescindible tener un sistema que controle cada característica de los sistemas tecnológicos. La monitorización de la carga de un SAI, los registros de los sistemas antivirus, el volumen de tráfico de la salida a Internet, la temperatura de los CPD, los elementos de seguridad de la red, la propia carga de CPU o Disco Duro de cualquier de los servidores que se tienen.

Estas aplicaciones deben tener un sistema de aviso ante cortes, pérdidas de servicio o fallas puntuales, pero además permitir la obtención de informes periódicos de cada uno de los elementos para tener un registro y prever de manera proactiva los cambios queden a lugar para evitar fallos posteriores que resultasen insalvables.

8.6. Gestión de Contraseñas.

El protocolo de generación y cambio de contraseñas críticas en un entorno corporativo. Se debe tener en cuenta que, con el tiempo, muchas contraseñas pasan por demasiadas manos, lo que puede suponer un problema de seguridad en las organizaciones. Cambiar periódicamente la contraseña de la wifi pública, activar la caducidad de las contraseñas de los usuarios del directorio activo y modificar las claves de los equipos en producción de vez en cuando, ayuda a que nuestros trabajadores tienen acceso únicamente a los recursos necesarios para su desempeño en cada una de sus labores.

Adicional es importante, que como avanza el tiempo la organización se suscribe a más y más servicios digitales que requieren un usuario o registro de login, donde es muy tentador que se use la misma contraseña y así no olvidarla, por los cual es un tremendo error. Las claves de acceso a equipos, correos electrónicos, archivos deben ser contraseñas robustas. Se debe evitar el uso de nombres comunes, fechas relevantes o de cumpleaños se recomienda construir varias contraseñas en las que usen minúsculas, mayúsculas, números y

caracteres especiales, no olvidar que es una buena práctica cambiarlas regularmente.

8.7. Gestión de Usuarios.

Las organizaciones no se dan de baja correctamente a los usuarios en los sistemas de información o queda algún usuario que no se tenía en cuenta en algún momento. No está de más programar informes que adviertan de usuarios inactivos en los sistemas y poder así eliminar o deshabilitar aquellas cuentas de acceso al servidor que no sean necesarias.

Se debe generar avisos mensuales de usuarios inactivos durante más de un mes. Así, con esta información puede valorar la necesidad de cursar la baja de estos, evitando tener cuentas en el sistema de usuarios inactivos de cualquier tipo, ya sean cuentas de usuario, de VPN o de algún aplicativo concreto.

8.8. Gestión de la Configuración (CMDB).

Es necesario tener las Bases de Datos de Gestión de Configuración (CMDB) de los activos de las organizaciones es una tarea tremendamente útil e importante, aunque sea algo tediosa y compleja. Además, es necesario ejecutar tareas periódicas para mantenerlas actualizadas lo más que se pueda, realizar auditorías, revisar los cambios, entradas y salidas de material, accesos y demás. Existen varias herramientas específicas que ayudan a llevar un buen mantenimiento de la CMDB en la organización.

Es vital mantener una base de datos actualizada y bien gestionada para afrontar cualquier situación tales como valorar accesos al entorno corporativo, encontrar rápidamente un equipo infectado o saber quién tiene acceso a cada recurso en la organización.

8.9. Revisión de Contratos/Mantenimientos/Licencias.

En las organizaciones se debe tener contratadas licencias o mantenimientos de los dispositivos para apoyo técnico o funcionalidades concretas. Es vital revisar constantemente la fecha de caducidad de estos, evitando así quedarse sin

soporte ante algún fallo o perdiendo acceso a algún aplicativo concreto por la falta de la licencia. No realizar esta revisión puede suponer una perdida en la producción, lo que puede acarrea en una pérdida económica innecesaria a la organización.

8.10. Pruebas de Planes de Contingencia.

Antes de que suceda cualquier emergencia, lo recomendable es realizar un análisis de riesgo y vulnerabilidad, conocer las fortalezas y debilidades de los equipos, la red interna, los servidores, las conexiones a Internet y demás dispositivos de la organización. Conociendo los riesgos y puntos débiles, es más fácil tomar decisiones en cuanto a las medidas de seguridad que se deben implementar y los protocolos a seguir en caso de que la información de la organización se vea comprometida.

Realizar simulacros en caso de desastre y así estar preparados ante cualquier emergencia que ocurra. Se debe probar a recuperar copias de seguridad, probar los equipos que se encuentren como respaldo, líneas secundarias para contingencia y demás herramientas que se utilizan para el desempeño diario de las tareas en la organización.

Con el fin de asegurar el éxito de los planes de contingencia, para ganar experiencia frente a estas situaciones o para medir tiempos de respuesta, es necesario realizar pruebas para comprobar que, en caso de un incidente grave, se pueda volver a la normalidad lo antes posible en la organización.

8.11. Firewall dedicado al entorno de la Organización

La instalación de un firewall físico en la red se conseguirá que el tráfico de datos habitual de la organización está monitorizado y filtrado adecuadamente, donde se implemente una política de bloqueo diseñada especialmente para cada red logrando minimizar los riesgos ante cualquier amenaza o ataque. Contar con un servidor propio, es recomendable si en la organización se usan más de cinco equipos de cómputo, ya que esto disminuye el riesgo de pérdida de archivos o información.

8.12. Precaución con las conexiones inalámbricas gratuitas o públicas

Es muy seductor utilizar conexiones Wifi-gratuitas ya sea en aeropuertos, restaurantes o lugares públicos. Aun así, se debe tener claro que al conectarnos a una red sin contraseña o de poca seguridad cualquier usuario malintencionado que también esté conectado podrá interceptar el tráfico de la información, logrando así copiar nuestras actividades y contraseñas. En estos casos se debe poner un cuidado especial con las conexiones remotas al ordenador del trabajo o de casa.

8.13. La información importante es mejor cifrada

En los ordenadores se tiene información importante que no puede ser ni leída ni vista sin autorización. Una manera segura de proteger la información de la organización ante una amenaza es utilizar aplicaciones de cifrado para la apertura y gestión. Los sistemas operativos habituales como son Windows o Mac vienen con potentes herramientas integradas para conseguir cifrar cada uno de los datos. Es bastante común que los teléfonos inteligentes o tabletas se pierdan o sean robados, para que no se tenga acceso a la información que contienen estos dispositivos, es importante que ésta se encuentre cifrada en cualquier momento.

8.14. Evita acceder a las webs importantes a través de enlaces

Al acceder a la web del Banco a través de un enlace de un correo se corre el riesgo de que ese enlace sea fraudulento y direccione a páginas falsas que intentarán capturar las contraseñas de los usuarios. Es así, aunque es bastante complicado, se podría dar el caso de que el navegador se infectara y el virus modificara los destinos a los que apuntan nuestra barra de marcadores. Se debe acceder siempre introduciendo la dirección o URL en la barra de direcciones, y comprueba que efectivamente se encuentra en el sitio que deseado.

8.15. Precaución con las descargas de archivos

Al descargar programas o archivos de Internet se debe estar seguros de que proceden de fuentes de calidad. Cualquier archivo que provenga de un sitio malintencionado podría infectar los equipos de la organización y tomar el control de este. Siempre páginas de total confianza, evitando los directorios de dudosa reputación, y en el caso de los Smartphones no instalar nada fuera de los típicos mercados de APPS de cada plataforma.

8.16. Sensibilización y capacitación de empleados.

Uno de los principales riesgos para la información de las organizaciones son las prácticas descuidadas de sus colaboradores al usar Internet. Estas prácticas incluyen abrir correos electrónicos con programas malintencionados, uso de Wifi libre el cual puede comprometer la transferencia de información e incluso la pérdida de dispositivos de almacenamiento, teléfonos inteligentes o tabletas que contienen información relevante o claves de acceso de la organización. Por esto es importante sensibilizarlos y capacitarlos sobre buenas prácticas en el uso de Internet y dispositivos que son usados a diario por cada uno de los colaboradores.

Las buenas prácticas en las organizaciones ayudan en mantener la seguridad de la información en todos sus niveles, desde los usuarios, pasando por las aplicaciones y sin olvidar el hardware, es así, que las grandes compañías invierten mucho de su presupuesto por salvaguardar la información.

Por lo anterior, las organizaciones PyMES en la actualidad deben empezar a contemplar una parte de su presupuesto anual para la seguridad de la información y generando las buenas prácticas en el manejo de la misma ya que esto evita que tenga grandes pérdidas económicas, adicional que su prestigio e imagen se vean afectados, y sin olvidar que pueden certificarse en la ISO/IEC 27001 lo que conlleva más responsabilidad y acceso a contratos con los clientes ya sean privados, gubernamentales y públicos.

Una vez estén estipuladas las buenas prácticas y las diferentes políticas que las organizaciones o PyMES van a manejar no se puede dejar de un lado y olvidarlas porque es claro que ellas no se manejan solas, los colaboradores y las áreas de tecnología deben trabajan conjuntadamente para que estas estén siempre al día y actualizadas, estén en constante supervisión por todos los miembros de la organización, donde el objetivo principal es evitar el robo de la información por parte de los cibercriminales.

9. RECOMENDACIONES

Las organizaciones en Colombia y en el mundo se ven enfrentadas a grandes retos cada día con los delincuentes del ciberespacio ya que estos van detrás de mucha información y de la forma de como vulnerar el sistema el cual se protege con bastante esfuerzo. Es por eso que las organizaciones no deben escatimar ningún recurso ya sea económico, tecnológico o humano para poder cuidar cada parte de la organización.

La generación de las diferentes políticas de seguridad de la información son un gran trabajo para poder minimizar los riesgos a los cuales están expuestas las organizaciones, pero no se puede dejar a un lado el eslabón más débil de la cadena que son los colaboradores, es allí donde se debe trabajar fuertemente para capacitar, concientizar en cada uno de los riesgos que pueden ocurrir en el robo de la información los cuales son generados por los ciberdelicuentes,

Por lo anterior, las organizaciones deben generar adicional a sus políticas teniendo en cuenta sus necesidades y el sector económico en el que se encuentran, los planes de contingencia que generen las organizaciones estás deben permitir seguir operando y no tener pérdidas económicas, mientras se descubren cada una de las vulnerabilidades que afectaron al sistema y consecuentemente corregirlos, es así, que estos planes son diseñados como herramientas para la continuidad del negocio y se debe tener en cuenta cada uno de los principios de la seguridad.

Como se menciona anteriormente la vulnerabilidad más latente de las organizaciones son los colaboradores, las áreas de tecnología deben trabajar fuertemente con cada una de las áreas, para que se realicen capacitaciones constantes, adicional realizar revisiones periódicas en la organización para que los colaboradores conozcan y que manejen las diferentes políticas de seguridad de la información las cuales fueron diseñadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información.

CONCLUSIONES

Las organizaciones no pueden dejar de lado cada uno de los activos de alto valor que tienen en cada una de sus sedes, es así, que se deben tener un mayor compromiso por el área de tecnología en evaluar constantemente y determinar el nivel de protección que tienen en la actualidad o si deben realizar alguna mejora constante.

En la generación de los análisis y gestión de los riesgos para las PyMES es muy importante que se debe contar con una metodología definida en la cual se puedan orientar y así mismo basar la organización, ya que es de vital importancia para el desarrollo de los diferentes riesgos que puedan ser localizados por el departamento de seguridad de la organización, es allí, donde los esfuerzos para poder evitar que las posibles vulnerabilidades que sean encontradas en las organizaciones deban ser atacadas y/o trabajas para que se minimice el riesgo a que ocurran.

En Colombia ya las organizaciones están trabajando para poder certificarse o acreditarse en la norma ISO 27001 – seguridad de la información pero también se basan en la familia completa de la 27000 y de la 31000 que es la que se encarga de la gestión de los riesgos pero a nivel general, es por eso que ya tener le certificado garantizan a los clientes que la información que se va a manejar va tener unos niveles de seguridad y así asegurar que esta no será ni otorgada y robada por algún delincuente cibernético.

Las diferentes alternativas que existen en el mercado para minimizar cada uno de los riesgos y ataques son muy importantes, pero cada una de las estrategias que se proponen sirven para ayudar a que las organizaciones tengan los riesgos ya sea económico y social al mínimo, y así no se vean afectados los diferentes intereses de las organizaciones

Para finalizar, las organizaciones que trabaja en el análisis y gestión de los riesgos tiene pocas probabilidades a que sean atacadas por los ciberdelincuentes, donde estos mismos atacan para poder apoderarse ya sea de

las cuentas bancarias o solo por fisgonear la información que manejan. Con las metodologías vistas y la combinación de un sin número de herramientas las organizaciones lo que pretenden es adelantarse a los ataques y poder cerrar la brecha a los delincuentes.

REFERENCIAS BIBLIOGRÁFICAS

AMUTIO GÓMEZ, Miguel Ángel, CANDAU, Javier y MAÑAS, José Antonio. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I, II y III. Madrid: Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica. 2012. NIPO: 630-12-171-8

BARRETO CUITIVA, Julián Hernán. Diseño de manual de diagnóstico y prevención de Vulnerabilidades en redes de datos para pymes. Proyecto de grado Seguridad Informática. Bogotá D.C.: Universidad Nacional Abierta y a Distancia. Escuela De Ciencias Básicas, Tecnología E Ingeniería. [consultado 10 de noviembre de 2.020]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/15026/80225921.pdf?sequence=1&isAllowed=y

BECERRA, Jairo, et al. LA SEGURIDAD EN EL CIBERESPACIO Un desafío para Colombia. Bogotá D.C., Gladys Elena Medina Ochoa, 2.019. ISBN-E: 978-958-52165-5-6

BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. [Sitio web]. ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? [consultado 29 de mayo de 2.020]. Disponible en https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

CASTRO, Alicia. Auditoría y Segurización de un Servidor Web. Proyecto de grado Seguridad Informática. Instituto Universitario Aeronáutico. [consultado 15 de diciembre de 2.020]. Disponible en https://rdu.iua.edu.ar/bitstream/123456789/1834/1/Informe_vfinal_CastroAlicia_1.pdf

COMPUTER IBIS. [Sitio web]. Madrid: IBIS. Buenas prácticas de Seguridad Informática. [consultado 6 de marzo de 2.021]. Disponible en https://www.ibiscomputer.com/blog/74-buenas-practicas-de-seguridad-informatica

FERNANDEZ, Yubal. [Sitios web]. ¿Cuál es la diferencia: ¿malware, virus, gusanos, spyware, troyanos, ransomware, etcétera? [consultado 28 de mayo de 2.020]. Obtenido de https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera

GONZÁLEZ AGUDELO, Daniel Felipe. El riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas BASC. Proyecto de grado en seguridad y salud ocupacional. Bogotá D.C.: Universidad Militar Nueva Granada. Facultad de relaciones internacionales, estrategia y seguridad administración de la seguridad y salud ocupacional. [consultado 28 de mayo de 2.020]. Disponible en

https://repository.unimilitar.edu.co/bitstream/handle/10654/12251/ENSAYO%20FINAL.pdf?sequence=1

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Decálogo de buenas prácticas de seguridad en un Departamento de Informática. [consultado 6 de marzo de 2.021]. Disponible en de https://www.incibe.es/protege-tu-empresa/blog/decalogo-buenas-practicas-seguridad-departamento-informatica

KALI LINUX. [Sitio web]. Kali Linux Tools Listing. [consultado 20 de marzo de 2.021]. Disponible en https://tools.kali.org/tools-listing

MIERES, Jorge. Buenas prácticas en seguridad informática. [En línea]. Estados Unidos de América. 2.009. Disponible en https://www.welivesecurity.com/wp-content/uploads/2014/01/buenas_practicas_seguridad_informatica.pdf

NOVOA, Helena Alemán, RODRIGUEZ BARRERA, Claudia. Metodologías para el análisis de riesgos en los SGSI. Revista Especializada en Ingeniería. [En Línea]. Bogotá (Colombia): Universidad Nacional Abierta y a Distancia, 22 de octubre de 2015. Vol. 9, pp 73 - 85. [consultado 28 de mayo de 2.020]. Disponible en https://doi.org/10.22490/25394088.1435

POLICÍA NACIONAL DE COLOMBIA. [Sitio web]. Boletín de análisis en Ciberseguridad Pyme. Centro Cibernético Policial. [consultado 04 de marzo de 2.020]. Disponible en https://caivirtual.policia.gov.co/sites/default/files/clientes_y_proveedores_0.pdf

OBS BUSINESS SCHOOL. [Sitio web]. ¿Qué es ciberseguridad y de qué fases consta? [consultado 08 de marzo de 2.020]. Disponible en https://obsbusiness.school/es/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta

OPENWEBINARS [Sitio web]. ¿Qué es la ciberseguridad?. [consultado 28 de mayo de 2.020]. Disponible en https://openwebinars.net/blog/que-es-la-ciberseguridad/

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. [Sitio web]. Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. [Consulta: 10 de abril de 2.020]. Disponible en http://sedici.unlp.edu.ar/bitstream/handle/10915/44143/OEA-_Tendencias_en_la_seguridad_cibern%C3%A9tica_en_Am%C3%A9rica_Latina_y_el_Caribe_y_respuestas_de_los_gobiernos__33_p._.pdf?sequence=19&isAllowed=y

OWASP. [Sitio web]. Top 10 Web Application Security Risks. [Consulta: 18 de abril de 2.021]. Disponible en https://owasp.org/www-project-top-ten/

RODRIGUEZ CARRILLO, Ana María. Análisis y diagnóstico de la seguridad informática de Indeportes Boyacá Universidad Nacional Abierta y a Distancia. Proyecto de grado Seguridad Informática. Bogotá D.C.: Universidad Nacional

Abierta y a Distancia. Escuela De Ciencias Básicas, Tecnología E Ingeniería. [consultado 10 de noviembre de 2.020]. Disponible en https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2692/5/53070244.pdf

TEAM. [Sitio web]. Las mejores medidas de Seguridad Informática. [consultado 04 de marzo de 2.020]. Disponible en https://www.teamnet.com.mx/blog/las-mejores-medidas-de-seguridad-informatica

TECHTARGET. [Sitio web]. Prueba de penetración (pen test). [consultado 08 de marzo de 2.020]. Disponible en https://searchdatacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test

SOLARTE SOLARTE, Francisco Nicolás, ENRIQUEZ ROSERO, Edgar Rodrigo y BENAVIDES, Mirian del Carmen. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL [En línea] Bogotá (Colombia): Universidad Nacional Abierta y a Distancia. 31 de diciembre de 2.015. Vol. 28 Núm. 5. pp 492-507. [consultado 28 de mayo de 2.020]. Disponible en http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

UNIVERSIDAD DE LOS ANDES. [Sitio web]. Simulacro de ataques a infraestructuras nacionales. [consultado 04 de marzo de 2.020]. Disponible en https://sistemas.uniandes.edu.co/en/component/k2/item/128-simulacro-de-ataques-a-infraestructuras-nacionales

Anexo 1. Tipos de Activos

Tipo	Nivel 1	Nivel 2	Nivel 3
[D] Datos / Información	[Files] Ficheros de datos		
	[backup] Copias de respaldo		
	[conf] Datos de configuración		
	[int] Datos de gestión interna		
	[password] Credenciales		
	[auth] Datos de validación de credenciales		
	[acl] Datos de control de acceso		
	[log] Registro de actividad (log)		
	[source] Código fuente		
	[exe] Código ejecutable		
	[test] Datos de prueba		
[K] Claves criptográficas	[info] Protección de la información	[encrypt] Claves de cifra	[shared_secret] secreto compartido
			[public_encryption] clave pública de cifra
			[public_decryption] clave privada de descifrado
		[sign] claves de firma	[shared_secret] secreto compartido
			[public_signature] clave privada de firma
			[public_verification] clave pública de verificación de firma
	[com] protección de las comunicaciones	[channel] claves de cifrado del canal	
		[authentication] claves de autenticación	

		[verification] claves de verificación de autenticación	
	[disk] cifrado de soportes de información	[encrypt] claves de cifra	
	[x509] certificados de clave pública		
[S] Servicios	[anon] anónimo		
	[pub] al público en general		
	[ext] a usuarios externos		
	[int] interno		
	[www] world wide web		
	[email] correo electrónico		
	[file] almacenamiento de ficheros		
	[ftp] transferencia de ficheros		
	[edi] intercambio electrónico de datos		
	[dir] servicio de directorio		
	[idm] gestión de identidades		
	[ipm] gestión de privilegios		
	[pki] PKI - infraestructura de clave pública		
[SW] Aplicaciones (Software)	[prp] desarrollo propio		
	[sub] desarrollo a medida		
	[std] estándar	[browser] navegador web	
		[www] servidor de presentación	
		[app] servidor de aplicaciones	
		[email_client] cliente de correo electrónico	

		[email_server] servidor de correo electrónico	
		[file] servidor de ficheros	
		[dbms] sistema de gestión de bases de datos	
		[tm] monitor transaccional	
		[office] ofimática	
		[av] anti virus	
		[os] sistema operativo	
		[hypervisor] gestor de máquinas virtuales	
		[ts] servidor de terminales	
		[backup] sistema de backup	
[HW] Equipos	[host] grandes equipos		
	[mid] equipos medios		
	[pc] informática personal		
	[mobile] informática móvil		
	[pda] agendas electrónicas		
	[vhost] equipo virtual		
	[backup] equipamiento de respaldo		
	[peripheral] periféricos	[print] medios de impresión	
		[scan] escáneres	
		[crypto] dispositivos criptográficos	
	[bp] dispositivo de frontera		
	[network] soporte de la red	[modem] módems	
		[hub] concentradores	
		[switch] conmutadores	
		[router] encaminadores	

		[bridge] pasarelas	
		[firewall] cortafuegos	
		[wap] punto de acceso inalámbrico	
	[pabx] centralita telefónica		
	[ipphone] teléfono IP		
[COM] Comunicaciones	[PSTN] red telefónica		
	[ISDN] rdsi		
	[X25] X25		
	[ADSL] ADSL		
	[pp] punto a punto		
	[switch]		
	[radio] comunicaciones radio		
	[wifi] red inalámbrica		
	[mobile] telefonía móvil		
	[sat] por satélite		
	[LAN] red local		
	[MAN] red metropolitana		
	[Internet] Internet		
[Media] Soportes de Información	[electronic] electrónicos	[disk] discos	
		[vdisk] discos virtuales	
		[san] almacenamiento en red	
		[disquette] disquetes	
		[cd] cederrón (CD-ROM)	
		[usb] memorias USB	
		[dvd] DVD	
		[tape] cinta magnética	
		[mc] tarjetas de memoria	
		[ic] tarjetas inteligentes	
	[non_electronic] no electrónicos	[printed] material impreso	

		[tape] cinta de papel	
		[film] microfilm	
		[cards] tarjetas perforadas	
[AUX] Elementos Auxiliares	[power] fuentes de alimentación		
	[ups] sistemas de alimentación ininterrumpida		
	[gen] generadores eléctricos		
	[ac] equipos de climatización		
	[cabling] cableado	[wire] cable eléctrico	
		[fiber] fibra óptica	
	[robot] robots	[tape] ... de cintas	
		[disk] ... de discos	
	[supply] suministros esenciales		
	[destroy] equipos de destrucción de soportes de información		
	[furniture] mobiliario: armarios, etc		
	[safe] cajas fuertes		
[L] Instalaciones	[site] recinto		
	[building] edificio		
	[local] cuarto		
	[mobile] plataformas móviles	[car] vehículo terrestre: coche, camión, etc.	
		[plane] vehículo aéreo: avión, etc.	
		[ship] vehículo marítimo: buque, lancha, etc.	
		[shelter] contenedores	
	[channel] canalización		
	[backup] instalaciones de respaldo		

[P] Personal	[ue] usuarios externos		
	[ui] usuarios internos		
	[op] operadores		
	[adm] administradores de sistemas		
	[com] administradores de comunicaciones		
	[dba] administradores de BBDD		
	[sec] administradores de seguridad		
	[des] desarrolladores / programadores		
	[sub] subcontratas		
	[prov] proveedores		

Anexo 2. Amenazas

AMENAZA	DESCRIPCION	ENBIOS
[N] Desastres naturales	[N.1] Fuego	01- INCENDIO
	[N.2] Daños por agua	02 - PERJUICIOS OCASIONADOS POR EL AGUA
	[N.*] Desastres naturales	03 – CONTAMINACIÓN
		04 - SINIESTRO MAYOR
		06 - FENÓMENO CLIMÁTICO
		07 - FENÓMENO SÍSMICO
		08 - FENÓMENO DE ORIGEN VOLCÁNICO
		09 - FENÓMENO METEOROLÓGICO
		10 - INUNDACIÓN
[I] De origen industrial	[I.1] Fuego	01- INCENDIO
	[I.2] Daños por agua	02 - PERJUICIOS OCASIONADOS POR EL AGUA
	[I.*] Desastres industriales	04 - SINIESTRO MAYOR
	[I.3] Contaminación mecánica	03 – CONTAMINACIÓN
	[I.4] Contaminación electromagnética	14 - EMISIONES ELECTROMAGNÉTICAS
		15- RADIACIONES TÉRMICAS
		16 - IMPULSOS ELECTROMAGNÉTICOS
	[I.5] Avería de origen físico o lógico	28 - AVERÍA DEL HARDWARE
		29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE
	[I.6] Corte del suministro eléctrico	12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA
	[I.7] Condiciones inadecuadas de temperatura o humedad	11- FALLAS EN LA CLIMATIZACIÓN
	[I.8] Fallo de servicios de comunicaciones	13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN
	[I.9] Interrupción de otros servicios y suministros esenciales	
	[I.10] Degradación de los soportes de almacenamiento de la información	28 - AVERÍA DEL HARDWARE
		29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE
	[I.11] Emanaciones electromagnéticas	17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	38 - ERROR DE USO

	[E.2] Errores del administrador	38 - ERROR DE USO
	[E.3] Errores de monitorización (log)	
	[E.4] Errores de configuración	
	[E.7] Deficiencias en la organización	
	[E.8] Difusión de software dañino	
	[E.9] Errores de re-encaminamiento	
	[E.10] Errores de secuencia	
	[E.14] Escapes de información	
	[E.15] Alteración accidental de la información	
	[E.18] Destrucción de información	
	[E.19] Fugas de información	
	[E.20] Vulnerabilidades de los programas (software)	
	[E.21] Errores de mantenimiento / actualización de programas (software)	31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE
		32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN
	[E.24] Caída del sistema por agotamiento de recursos	30 - SATURACIÓN DEL SISTEMA INFORMÁTICO
	[E.25] Pérdida de equipos	22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS
	[E.28] Indisponibilidad del personal	42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	
	[A.4] Manipulación de la configuración	
	[A.5] Suplantación de la identidad del usuario	40 - USURPACIÓN DE DERECHO
	[A.6] Abuso de privilegios de acceso	39 - ABUSO DE DERECHO
	[A.7] Uso no previsto	

	[A.8] Difusión de software dañino	
	[A.9] Re-encaminamiento de mensajes	
	[A.10] Alteración de secuencia	36 - ALTERACIÓN DE DATOS
	[A.11] Acceso no autorizado	33 - USO ILÍCITO DEL HARDWARE
	[A.12] Análisis de tráfico	
	[A.13] Repudio	41 - NEGACIÓN DE ACCIONES
	[A.14] Interceptación de información (escucha)	19 - ESCUCHA PASIVA
	[A.15] Modificación deliberada de la información	
	[A.18] Destrucción de información	
	[A.19] Divulgación de información	23 – DIVULGACIÓN
		27 – GEOLOCALIZACIÓN
		34 - COPIA ILEGAL DE SOFTWARE
	[A.22] Manipulación de programas	26 - ALTERACIÓN DE PROGRAMAS
	[A.23] Manipulación de los equipos	25 - SABOTAJE DEL HARDWARE
	[A.24] Denegación de servicio	30 - SATURACIÓN DEL SISTEMA INFORMÁTICO
	[A.25] Robo	20 - ROBO DE SOPORTES O DOCUMENTOS
		21 - ROBO DE HARDWARE
	[A.26] Ataque destructivo	05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES
	[A.27] Ocupación enemiga	
	[A.28] Indisponibilidad del personal	42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL
	[A.29] Extorsión	
	[A.30] Ingeniería social (picaresca)	

Anexo 3. Salvaguardas

Salvaguarda	Abreviatura	Significado
Protecciones generales u horizontales	H	Protecciones Generales
	H.IA	Identificación y autenticación
	H.AC	Control de acceso lógico
	H.ST	Segregación de tareas
	H.IR	Gestión de incidencias
	H.tools	Herramientas de seguridad
	H.tools.AV	Herramienta contra código dañino
	H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión
	H.tools.CC	Herramienta de chequeo de configuración
	H.tools.VA	Herramienta de análisis de vulnerabilidades
	H.tools.TM	Herramienta de monitorización de tráfico
	H.tools.DLP	DLP: Herramienta de monitorización de contenidos
	H.tools.LA	Herramienta para análisis de logs
	H.tools.HP	Honey net / honey pot
	H.tools.SFV	Verificación de las funciones de seguridad
	H.VM	Gestión de vulnerabilidades
	H.AU	Registro y auditoría
Protección de los datos / información	D	Protección de la Información
	D.A	Copias de seguridad de los datos (backup)
	D.I	Aseguramiento de la integridad
	D.C	Cifrado de la información
	D.DS	Uso de firmas electrónicas
	D.TS	Uso de servicios de fechado electrónico (time stamping)
Protección de las claves criptográficas	K	Gestión de claves criptográficas
	K.IC	Gestión de claves de cifra de información
	K.DS	Gestión de claves de firma de información
	K.disk	Gestión de claves para contenedores criptográficos
	K.comms	Gestión de claves de comunicaciones
	K.509	Gestión de certificados
Protección de los servicios	S	Protección de los Servicios
	S.A	Aseguramiento de la disponibilidad
	S.start	Aceptación y puesta en operación
	S.SC	Se aplican perfiles de seguridad
	S.op	Explotación
	S.CM	Gestión de cambios (mejoras y sustituciones)
	S.end	Terminación
	S.www	Protección de servicios y aplicaciones web

	S.email	Protección del correo electrónico
	S.dir	Protección del directorio
	S.dns	Protección del servidor de nombres de dominio (DNS)
	S.TW	Teletrabajo
	S.voip	Voz sobre IP
Protección de las aplicaciones (software)	SW	Protección de las Aplicaciones Informáticas
	SW.A	Copias de seguridad (backup)
	SW.start	Puesta en producción
	SW.SC	Se aplican perfiles de seguridad
	SW.op	Explotación / Producción
	SW.CM	Cambios (actualizaciones y mantenimiento)
	SW.end	Terminación
Protección de los equipos (hardware)	HW	Protección de los Equipos Informáticos
	HW.start	Puesta en producción
	HW.SC	Se aplican perfiles de seguridad
	HW.A	Aseguramiento de la disponibilidad
	HW.op	Operación
	HW.CM	Cambios (actualizaciones y mantenimiento)
	HW.end	Terminación
	HW.PCD	Informática móvil
	HW.print	Reproducción de documentos
	HW.pabx	Protección de la centralita telefónica (PABX)
Protección de las comunicaciones	COM	Protección de las Comunicaciones
	COM.start	Entrada en servicio
	COM.SC	Se aplican perfiles de seguridad
	COM.A	Aseguramiento de la disponibilidad
	COM.aut	Autenticación del canal
	COM.I	Protección de la integridad de los datos intercambiados
	COM.C	Protección criptográfica de la confidencialidad de los datos intercambiados
	COM.op	Operación
	COM.CM	Cambios (actualizaciones y mantenimiento)
	COM.end	Terminación
	COM.internet	Internet: uso de acceso
	COM.wifi	Seguridad Wireless (WiFi)
	COM.mobile	Telefonía móvil
	COM.DS	Segregación de las redes en dominios
Protección en los puntos de interconexión con otros sistemas	IP	Puntos de interconexión: conexiones entre zonas de confianza
	IP.SPP	Sistema de protección perimetral
	IP.BS	Protección de los equipos de frontera
	MP	Protección de los Soportes de Información

Protección de los soportes de información	MP.A	Aseguramiento de la disponibilidad
	MP.IC	Protección criptográfica del contenido
	MP.clean	Limpieza de contenidos
	MP.end	Destrucción de soportes
Protección de los elementos auxiliares	AUX	Elementos Auxiliares
	AUX.A	Aseguramiento de la disponibilidad
	AUX.start	Instalación
	AUX.power	Suministro eléctrico
	AUX.AC	Climatización
	AUX.wires	Protección del cableado
Seguridad física – Protección de las instalaciones	L	Protección de las Instalaciones
	L.design	Diseño
	L.depth	Defensa en profundidad
	L.AC	Control de los accesos físicos
	L.A	Aseguramiento de la disponibilidad
	L.end	Terminación
Salvaguardas relativas al personal	PS	Gestión del Personal
	PS.AT	Formación y concienciación
	PS.A	Aseguramiento de la disponibilidad
Salvaguardas de tipo organizativo	G	Organización
	G.RM	Gestión de riesgos
	G.plan	Planificación de la seguridad
	G.exam	Inspecciones de seguridad
Continuidad de operaciones	BC	Continuidad del negocio
	BC.BIA	Análisis de impacto (BIA)
	BC.DRP	Plan de Recuperación de Desastres (DRP)
Externalización	E	Relaciones Externas
	E.1	Acuerdos para intercambio de información y software
	E.2	Acceso externo
	E.3	Servicios proporcionados por otras organizaciones
	E.4	Personal subcontratado
Adquisición y desarrollo	NEW	Adquisición / desarrollo
	NEW.S	Servicios: Adquisición o desarrollo
	NEW.SW	Aplicaciones: Adquisición o desarrollo
	NEW.HW	Equipos: Adquisición o desarrollo
	NEW.COM	Comunicaciones: Adquisición o contratación
	NEW.MP	Soportes de Información: Adquisición
	NEW.C	Productos certificados o acreditados

Anexo 4. Controles ISO 27000

Dominio	Objetivo del Control	Control
A.5 Políticas de seguridad de la información	A.5.1 Directrices de gestión de la seguridad de la información	A.5.1.1 Políticas para la seguridad de la información
		A.5.1.2 Revisión de las políticas para la seguridad de la información
A.6 Organización de la seguridad de la información	A.6.1 Organización interna	A.6.1.1 Roles y responsabilidades en seguridad de la información
		A.6.1.2 Segregación de tareas
		A.6.1.3 Contacto con las autoridades
		A.6.1.4 Contacto con grupos de interés especial
		A.6.1.5 Seguridad de la información en la gestión de proyectos
	A.6.2 Los dispositivos móviles y el teletrabajo	A.6.2.1 Política de dispositivos móviles
		A.6.2.2 Teletrabajo
A.7 Seguridad relativa a los recursos humanos	A.7.1 Antes del empleo	A.7.1.1 Investigación de antecedentes
		A.7.1.2 Términos y condiciones del empleo
	A.7.2 Durante el empleo	A.7.2.1 Responsabilidades de gestión
		A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
		A.7.2.3 Proceso disciplinario
	A.7.3 Finalización del empleo o cambio en el puesto de trabajo	A.7.3.1 Responsabilidades ante la finalización o cambio
A.8 Gestión de activos	A.8.1 Responsabilidad sobre los activos	A.8.1.1 Inventario de activos
		A.8.1.2 Propiedad de los activos
		A.8.1.3 Uso aceptable de los activos

		A.8.1.4 Devolución de activos
	A.8.2 Clasificación de la información	A.8.2.1 Clasificación de la información
		A.8.2.2 Etiquetado de la información
		A.8.2.3 Manipulado de la información
	A.8.3 Manipulación de los soportes	A.8.3.1 Gestión de soportes extraíbles
		A.8.3.2 Eliminación de soportes
		A.8.3.3 Soportes físicos en tránsito
A.9 Control de acceso	A.9.1 Requisitos de negocio para el control de acceso	A.9.1.1 Política de control de acceso
		A.9.1.2 Acceso a las redes y a los servicios de red
	A.9.2 Gestión de acceso de usuario	A.9.2.1 Registro y baja de usuario
		A.9.2.2 Provisión de acceso de usuario
		A.9.2.3 Gestión de privilegios de acceso
		A.9.2.4 Gestión de la información secreta de autenticación de los usuarios
		A.9.2.5 Revisión de los derechos de acceso de usuario
		A.9.2.6 Retirada o reasignación de los derechos de acceso
	A.9.3 Responsabilidades del usuario	A.9.3.1 Uso de la información secreta de autenticación
	A.9.4 Control de acceso a sistemas y aplicaciones	A.9.4.1 Restricción del acceso a la información
		A.9.4.2 Procedimientos seguros de inicio de sesión
		A.9.4.3 Sistema de gestión de contraseñas
		A.9.4.4 Uso de utilidades con privilegios del sistema

		A.9.4.5 Control de acceso al código fuente de los programas
A.10 Criptografía	A.10.1 Controles criptográficos	A.10.1.1 Política de uso de los controles criptográficos
		A.10.1.2 Gestión de claves
A.11 Seguridad física y del entorno	A.11.1 Áreas seguras	A.11.1.1 Perímetro de seguridad física
		A.11.1.2 Controles físicos de entrada
		A.11.1.3 Seguridad de oficinas, despachos y recursos
		A.11.1.4 Protección contra las amenazas externas y ambientales
		A.11.1.5 El trabajo en áreas seguras
		A.11.1.6 Áreas de carga y descarga
	A.11.2 Seguridad de los equipos	A.11.2.1 Emplazamiento y protección de equipos
		A.11.2.2 Instalaciones de suministro
		A.11.2.3 Seguridad del cableado
		A.11.2.4 Mantenimiento de los equipos
		A.11.2.5 Retirada de materiales propiedad de la empresa
		A.11.2.6 Seguridad de los equipos fuera de las instalaciones
		A.11.2.7 Reutilización o eliminación segura de equipos
		A.11.2.8 Equipo de usuario desatendido
		A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia

A.12 Seguridad de las operaciones	A.12.1 Procedimientos y responsabilidades operacionales	A.12.1.1 Documentación de procedimientos operacionales
		A.12.1.2 Gestión de cambios
		A.12.1.3 Gestión de capacidades
		A.12.1.4 Separación de los recursos de desarrollo, prueba y operación
	A.12.2 Protección contra el software malicioso (malware)	A.12.2.1 Controles contra el código malicioso
	A.12.3 Copias de seguridad	A.12.3.1 Copias de seguridad de la información
	A.12.4 Registros y supervisión	A.12.4.1 Registro de eventos
		A.12.4.2 Protección de la información del registro
		A.12.4.3 Registros de administración y operación
		A.12.4.4 Sincronización del reloj
	A.12.5 Control del software en explotación	A.12.5.1 Instalación del software en explotación
	A.12.6 Gestión de la vulnerabilidad técnica	A.12.6.1 Gestión de las vulnerabilidades técnicas
		A.12.6.2 Restricción en la instalación de software
	A.12.7 Consideraciones sobre la auditoria de sistemas de información	A.12.7.1 Controles de auditoría de sistemas de información
A.13 Seguridad de las comunicaciones	A.13.1 Gestión de la seguridad de las redes	A.13.1.1 Controles de red
		A.13.1.2 Seguridad de los servicios de red
		A.13.1.3 Segregación en redes
	A.13.2 Intercambio de información	A.13.2.1 Políticas y procedimientos de intercambio de información

		A.13.2.2 Acuerdos de intercambio de información
		A.13.2.3 Mensajería electrónica
		A.13.2.4 Acuerdos de confidencialidad o no revelación
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	A.14.1 Requisitos de seguridad en los sistemas de información	A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información
		A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas
		A.14.1.3 Protección de las transacciones de servicios de aplicaciones
	A.14.2 Seguridad en el desarrollo y en los procesos de soporte	A.14.2.1 Política de desarrollo seguro
		A.14.2.2 Procedimiento de control de cambios en sistemas
		A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
		A.14.2.4 Restricciones a los cambios en los paquetes de software
		A.14.2.5 Principios de ingeniería de sistemas seguros
		A.14.2.6 Entorno de desarrollo seguro
		A.14.2.7 Externalización del desarrollo de software
		A.14.2.8 Pruebas funcionales de seguridad de sistemas
		A.14.2.9 Pruebas de aceptación de sistemas
	A.14.3 Datos de prueba	A.14.3.1 Protección de los datos de prueba
A.15 Relación con proveedores	A.15.1 Seguridad en las relaciones con proveedores	A.15.1.1 Política de seguridad de la información en las

		relaciones con los proveedores
		A.15.1.2 Requisitos de seguridad en contratos con terceros
		A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones
	A.15.2 Gestión de la provisión de servicios del proveedor	A.15.2.1 Control y revisión de la provisión de servicios del proveedor
		A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes de seguridad de la información y mejoras	A.16.1.1 Responsabilidades y procedimientos
		A.16.1.2 Notificación de los eventos de seguridad de la información
		A.16.1.3 Notificación de puntos débiles de la seguridad
		A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
		A.16.1.5 Respuesta a incidentes de seguridad de la información
		A.16.1.6 Aprendizaje de los incidentes de seguridad de la información
		A.16.1.7 Recopilación de evidencias
A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	A.17.1 Continuidad de la seguridad de la información	A.17.1.1 Planificación de la continuidad de la seguridad de la información
		A.17.1.2 Implementar la continuidad de la seguridad de la información
		A.17.1.3 Verificación, revisión y evaluación de

		la continuidad de la seguridad de la información
	A.17.2 Redundancias	A.17.2.1 Disponibilidad de los recursos de tratamiento de la información
A.18 Cumplimiento	A.18.1 Cumplimiento de los requisitos legales y contractuales	A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
		A.18.1.2 Derechos de Propiedad Intelectual (DPI)
		A.18.1.3 Protección de los registros de la organización
		A.18.1.4 Protección y privacidad de la información de carácter personal
		A.18.1.5 Regulación de los controles criptográficos
	A.18.2 Revisiones de la seguridad de la información	A.18.2.1 Revisión independiente de la seguridad de la información
		A.18.2.2 Cumplimiento de las políticas y normas de seguridad
		A.18.2.3 Comprobación del cumplimiento técnico