Análisis, valoración de riesgos y controles de ciberseguridad.

Breve descripción:

A partir del estudio de este componente formativo, el aprendiz estará en capacidad describir y aplicar las acciones de análisis y valoración de riesgos y controles de ciberseguridad; todo ello con base en métodos específicos de análisis de riesgos de seguridad. Adicionalmente, podrá establecer como resultado, el plan de tratamiento adecuado.

Noviembre 2023

Tabla de contenido

Introducción

Una cordial bienvenida a este componente formativo, en el cual se podrán reconocer e identificar las acciones de análisis y valoración de riesgos y controles de ciberseguridad.

Para comenzar, se debe revisar el siguiente recurso:

Video 1. Introducción

Enlace de reproducción del video

Síntesis del video: Introducción
Los análisis de riesgos en seguridad de la información se basan en metodologías de riesgo existentes, las cuales sientan la base para realizar las valoraciones apropiadas, según el contexto y objetivos que se pretendan. Un análisis de riesgos en ciberseguridad es similar al análisis de riesgos de seguridad de la información.

Se hace fundamental, comprender que la ciberseguridad se enfoca en la seguridad de la información en el ciberespacio, en el mundo digital o cibernético, pero que también abarca aspectos de la geopolítica y la sociedad.

En este componente de formación se darán a conocer las dinámicas para realizar un análisis y valoración de riesgos y controles de ciberseguridad con base en métodos de análisis de riesgos de seguridad que permiten tener los conocimientos fundamentales para realizar un plan de tratamiento de riesgos bien fundamentado.

Tenga presente:

- ✓ Explorar todos los recursos didácticos que el componente tiene para usted.
- ✓ Procurar llevar un registro de los elementos teóricos, conceptuales y prácticos que va asimilando en el recorrido del componente. Para ello, tenga a la mano una herramienta de registro: computadora, libreta de notas o cualquier otra que le permita llevar apuntes.
- ✓ Seleccionar un buen momento y un espacio oportuno para el estudio de este componente.

1. Técnicas de recolección de información

Las técnicas de recolección de información involucran los métodos para la captura o toma de datos que se pueden aplicar en las investigaciones o procesos de una organización, los mismos se pueden dar en forma cualitativa o cuantitativa. Es importante resaltar que en la recolección de la información se debe validar la calidad de la información y sus fuentes.

En la recolección de información es importante tener claridad en algunos conceptos que orientan dicho proceso. A continuación, se presentan los más destacados, para asimilarlos mejor se recomienda llevar registro de ellos en la libreta de apuntes personal:

- ✓ **Información primaria:** es la información que se recolecta directamente, por medio de un sujeto directo con su objeto de investigación.
- ✓ **Información secundaria:** es aquella que se recopila con base en investigaciones realizadas o fuentes de información con propósitos diferentes. La información secundaria es recolectada sin tener contacto directo con el objeto de análisis.
- ✓ **Objeto:** elemento, proceso, área que puede ser objeto de interacción, análisis e investigación por uno o más individuos.
- ✓ **Sujeto:** actor o individuo que interactúa o participa con un objeto.

1.1. Técnicas de recolección más usuales

Para el proceso de recolección de la información, con fines de análisis y valoración de riesgos en ciberseguridad, existen distintas técnicas. Estas técnicas de recolección de información pueden ser aplicadas en diversos ámbitos y contextos. Tener un conocimiento suficiente de las mismas es importante para levantar los datos e información necesarios, que aseguren un proceso de análisis de riesgos de ciberseguridad más efectivo y cierto.

Para profundizar en las técnicas de recolección más usuales, se encontrará una explicación con detalle en el siguiente recurso:

Afiance los aspectos más importantes de este punto, explorando conscientemente el recurso que aquí le presentamos; recuerde llevar registro en su libreta personal de apuntes. ¡Adelante!

Enlace documento

1.2. Características de las técnicas de recolección

Las técnicas de recolección de información, en el proceso de análisis, valoración de riesgos y controles de ciberseguridad, tienen ciertas características o particularidades que, no solo las diferencias de las técnicas de recolección de otros procesos, sino que, además, favorecen la operación de quienes están a cargo de dicha tarea.

Las técnicas de recolección de información pueden apropiar las características que se descubrirán en el recurso que se muestra a continuación. ¡Adelante!

- **Técnicas Cualitativas:** pueden presentar alto nivel de entendimiento de los datos e información. La relevancia está dada en las respuestas individuales y su nivel de profundidad. Tienen un alto nivel de subjetividad y dependen del conocimiento, experiencia y percepción que un sujeto tiene sobre el objeto de estudio.
- **Técnicas Cuantitativas**

  Su base fundamental son los datos numéricos, que representan características o detalles particulares de un objeto de estudio. Una gran cantidad de datos sobre uno o más atributos, de un objeto de estudio, que permita generalizar en los resultados obtenidos, facilitando la comprensión y toma la de decisiones.
- **Registro de datos:** consiste en el proceso de recopilar los datos o información obtenida, cuando se aplican las técnicas de recolección de información. Este es un elemento importante que puede ser aplicado tanto en papel y archivos físicos, como en medios digitales, tales como: documentos de procesadores de texto, registros multimedia (imagen, audio, video), aplicaciones de software y bases de datos digitales.

2. Vulnerabilidades y amenazas

En la determinación de riesgos de ciberseguridad es importante comprender los conceptos de vulnerabilidad y amenaza, entendiendo que una o más amenazas pueden aprovechar una o más vulnerabilidades; generando riesgos en la confidencialidad, la integridad y la disponibilidad de la información, principios elementales de la seguridad de la información.

Para ampliar los conocimientos en lo referente a amenazas y vulnerabilidades, se debe explorar el recurso que se propone a continuación:

Video 2. Vulnerabilidades y amenazas

Enlace de reproducción del video

Síntesis del video: Vulnerabilidades y amenazas

Vulnerabilidades y amenazas: son elementos fundamentales de la seguridad de la información. Esta puede verse afectada negativamente por las amenazas y las vulnerabilidades. Pero ¿qué son? ¿Cómo afectan? ¿Qué es importante definir y entender de ellas?

Vulnerabilidades: se trata de aquella debilidad o fallo de seguridad que se presenta en un sistema de información, que puede estar compuesto por *software, hardware* y otros componentes y servicios tecnológicos, generando riesgos de seguridad de la información.

Las vulnerabilidades pueden ser aprovechadas por acciones no deliberadas, como errores humanos y fallos técnicos no intencionados. También, pueden ser explotadas por acciones intencionadas de atacantes internos o externos.

Se pueden presentar en diversos elementos o activos de información, tales como el Software, el Hardware, las personas, la infraestructura, las redes, las bases de datos, y otros tipos de activos relacionados.

Amenazas: es toda aquella acción o serie de acciones, que aprovechan las vulnerabilidades para romper la seguridad de los sistemas.

Una amenaza genera un efecto negativo, el cual puede entenderse como un impacto adverso; resultado de la violación de los principios de seguridad de la información.

Las fuentes comunes de amenazas de ciberseguridad suelen ser el malware o código malicioso, la ingeniería social, las amenazas persistentes avanzadas *APT, y* las *Botnets.*

2.1. Valoración de amenazas y vulnerabilidades

La valoración de amenazas y vulnerabilidades se puede realizar de manera conjunta, agrupando las mismas en riesgos de ciberseguridad y determinando la probabilidad de ocurrencia de dichos riesgos.

A través de las siguientes variantes se puede hacer la valoración pertinente de las amenazas y vulnerabilidades:

a) Probabilidad de ocurrencia

La valoración se puede dar de manera cualitativa y cuantitativa, por lo general se realiza de manera cualitativa definiendo escalas nominales con referencias numéricas que facilitan los cruces con otras características del análisis de riesgo de ciberseguridad, ver tabla 1.

Tabla 1. Probabilidad de ocurrencia.

MA	Muy alta	Casi seguro	5
A	Alta	Muy alto	4
M	Media	Posible	3
B	Baja	Poco probable	2

MB	Muy baja	Muy raro	1

Nota. Tomado de MAGERIT (2012).

b) Inventario de amenazas y vulnerabilidades

Para poder valorar la probabilidad de vulnerabilidades y amenazas hay que condensarlas en riesgos, por medio de un inventario de amenazas y elementos vulnerables asociados. Una representación puede ser como se muestra en la siguiente tabla 2:

Tabla 2. Inventario de amenazas y vulnerabilidades.

AMENAZA	TIPO	Tipo de activos que afecta			Dimensiones que afecta			Elementos vulnerables asociados		
		SW	HW	...	Confidencialidad	INTEGRIDAD	DISPONIBILIDAD	HW	SW	...
Ataque cibernético	Intencionado	X	na	...	X	X	X	na	X	...
...	...	...	...	...	...	...	...	...	...	...

Nota. Tomado de MAGERIT (2012).

c) Valoración de riesgos

La evaluación de riesgos de ciberseguridad que agrupa amenazas y vulnerabilidades de activos de información se realiza considerando el contexto y el tipo de activo de información, así entonces se puede considerar la siguiente tabla 3 de valoración:

Tabla 3. Valoración de riesgos

Activo de información	Tipo	Riesgo 1	Riesgo 1	Riesgo 2	Riesgo 2	Riesgo 3	Riesgo 3	Riesgo 4	Riesgo 4
		Probabilidad	valor	P	V	P	V	P	V
Servidor Web	Hardware	MA	5	M	3	A	4	...	...
Aplicación	Software	A	4	B	2	M	3	...	...
Internet	Servicio	No Aplica	NA	A	4	MB	1	...	...

Nota. Tomado de MAGERIT (2012).

2.2. Tratamiento de riesgos

El tratamiento de riesgos de ciberseguridad consiste en una serie de actividades en donde se aplican políticas y controles de seguridad digital a los riesgos críticos resultantes del proceso de análisis de riesgos. En un análisis de riesgos, se debe

desarrollar un plan de tratamiento de riesgos **PTR**, en donde se especifiquen los activos de información con los riesgos más críticos y las actividades que se deben desarrollar para mitigar los riesgos.

Las características que se deben considerar para realizar un plan de tratamiento de riesgos son:

- Activos de información con riesgos críticos.
- Riesgos asociados al activo.
- Causas de los riesgos.
- Controles aplicados.
- Tipo de tratamiento que se debe dar: mitigar o reducir el riesgo, evitar el riesgo, compartir o transferir el riesgo.
- Actividades a realizar para tratar el riesgo.
- Responsable por cada actividad.
- Prioridad de ejecución.
- Fecha de implementación.
- Observaciones.

Es importante destacar que para tratar un riesgo se debe implementar controles de ciberseguridad o fortalecer los existentes asociados al riesgo. Esto permite la mitigación del riesgo ya que los controles bien aplicados logran disminuir la probabilidad o impacto de los riesgos.

3. Seguridad e infraestructura de hardware y software

La infraestructura tecnológica es parte esencial para las operaciones de las organizaciones, las mismas pueden soportar herramientas para la gestión, planificación, ejecución y monitoreo de productos o servicios. Desde aplicaciones y servicios para la comunicación, hasta complejos sistemas para la toma de decisiones, como los Enterprise Resource Planning ERP o los aplicativos de inteligencia de negocios (business intelligence - BI).

La infraestructura tecnológica principalmente está compuesta por hardware y software, y es importante mencionar que para la misma es necesario aplicar una serie de buenas prácticas y/o controles de seguridad digital que permitan lograr que la misma sea segura y confiable.

3.1. Infraestructura de hardware y software

La infraestructura tecnológica consiste en los componentes de hardware y software requeridos para gestionar y operar entornos tecnológicos, que pueden ser implementados en instalaciones de la organización o en sistemas en la nube, Cloud Computing.

Se presentan a continuación, aspectos claves de la infraestructura de hardware y software; se deben estudiar atentamente y llevar registro de ello en la libreta personal de apuntes. ¡Adelante!

a) **Infraestructura tradicional:** “Una infraestructura de TI tradicional incluye los componentes de hardware y software habituales: instalaciones, centros de datos, servidores, computadores de escritorio de hardware de red y soluciones empresariales de software de aplicaciones.

   Normalmente, esta infraestructura requiere más energía, espacio físico y dinero que otros tipos de infraestructura. Se instala localmente para uso exclusivo, o privado, de la empresa.” (IBM, 2021)

b) **Infraestructura de la nube:** “Una infraestructura de TI en la nube es similar a la infraestructura tradicional. Sin embargo, los usuarios finales pueden accederla a través de Internet y tienen la capacidad de usar la virtualización para ocupar recursos informáticos sin realizar instalaciones locales.
   La virtualización conecta los servidores físicos de un proveedor de servicios en cualquier ubicación geográfica. Luego, divide y extrae los recursos, como el almacenamiento, para ponerlos a disposición de los usuarios, prácticamente en cualquier lugar donde haya conexión a Internet. Debido a que la infraestructura en la nube es a menudo pública, normalmente se conoce como una nube pública.” (IBM, 2021)

c) **Principales características de las infraestructuras**

   - Composición por elementos de hardware y software.
   - Comunicación por servicios de red basados hardware y software.
   - Segmentación de zonas, que pueden ser campus o red de usuarios e invitados, Demilitarized Zone - DMZ; bases de datos, servidores.

- Alta Disponibilidad en componentes, principalmente en los componentes de red, servidores de aplicación, storage y energía.
- Virtualización; Implementación de múltiples servidores virtuales en hiper visores tales como; VMware, Proxmox, XenServer, Citrix, Hyper-v, ESX.
- Implementación de Servidores de aplicación web y servicios; File.
- Transfer Protocol - FTP, Sistema de Nombres de Dominio DNS.
- Sistemas ERP, BI, entre otros.

d) **Infraestructura y seguridad:** la seguridad juega un papel muy importante en la infraestructura tecnológica y es parte de la misma, pues ésta se integra en componentes que permiten la protección de los datos en la red, servidores, aplicaciones y servicios tecnológicos.

e) **Controles de seguridad:** la seguridad, permite la protección de las infraestructuras, a través de algunos controles como los siguientes:

- Establecimiento de políticas y procedimientos de seguridad digital.
- Direccionamiento par el cumplimiento de la legislación aplicable en relación a las operaciones de la infraestructura tecnológica.
- Protección de dispositivos finales, hosts.
- Protección criptográfica.
- Seguridad física y del entorno.
- Copias de respaldo.
- Gestión de incidentes de seguridad digital; vulnerabilidades, eventos e incidentes.
- Entrenamiento y concienciación en ciberseguridad.

3.2. Componentes de infraestructura y seguridad

La infraestructura y seguridad cuentan con diversos componentes que interactúan entre sí y que son finalmente, los que constituyen la infraestructura tecnológica. Los componentes de seguridad a su vez son componentes de infraestructura, pero se convierten en elementos muy importantes que salvaguardan otros componentes de infraestructura y por eso toman una mayor relevancia.

Se debe explorar el recurso que se muestra a continuación y conocer las listas de componentes relacionados con infraestructura y seguridad:

1. **Componentes de infraestructura, más comunes**
   - **Servidores:** red, aplicación, servicios, bases de datos.
   - **Router:** enrutadores de red.
   - **Switch:** switches conectores de diversas capas de red.
   - **Sistema de refrigeración.**
   - **Storage:** sistemas de almacenamiento en red, network attached storage - nas.
   - **Cableado estructurado.**
2. **Otros componentes importantes de infraestructura**
   - **Potencia y energía:** sistemas de regulación de la energía, plantas eléctricas para redundancia.
   - **Equipos, computadores.**
   - **Periféricos:** Impresoras, escáneres, lectores láser, entre otros.

- **Software de virtualización:** VMware, Proxmox, XenServer, Citrix, Hyper-v, ESX.
- **Software de monitoreo:** monitoreo de red, capacidades y temperaturas.

3. **Componentes de seguridad más usuales**
   - **Firewall de Red:** asegura el entorno de conexión.
   - **Antimalware.**
   - **Firewall de aplicación.**
   - **IP Tables:** reglas de acceso en red.
   - **Sistemas** de correlación de eventos o Logs, Security Information and Event Management - SIEM.
   - **Cifrad**: conectividad y datos.
4. **Otros componentes importantes de la seguridad**
   - **VPN:** conexiones remotas seguras.
   - **IDS/IPS**: sistema de Detección y prevención de intrusiones.
   - **NIDS - Network Intrusion Detection System,** Sistemas de detección de intrusos en red.
   - **Herramientas de análisis de vulnerabilidades:** OpenVas, Nessus.
   - **WAF - Web Aplication Firewall, Firewall de aplicación**.
   - **DLP – Data Loss Prevention:** sistema de prevención de pérdida de datos o fuga de información.

3.3. Interconexiones de redes y seguridad perimetral

Hablar de interconexiones de redes y seguridad perimetral, es referirse a las conexiones de red entre los diferentes dispositivos, de acuerdo con los fundamentos de red o networking, incluyendo los dispositivos de seguridad perimetral.

Para una mejor comprensión de este punto, se debe estudiar atentamente la imagen animada que se muestra en pantalla (ver figura1) y tomar nota de los aspectos que ella explica:

Afiance los aspectos más importantes de este punto, explorando conscientemente el recurso que aquí le presentamos; recuerde llevar registro en su libreta personal de apuntes. ¡Adelante!

4. Herramientas de análisis de seguridad digital

Dentro de los controles de seguridad digital existen diversas herramientas para el análisis de la seguridad digital, las mismas permiten realizar diagnósticos del estado de la seguridad en los componentes de infraestructura de hardware y software.

Algunas herramientas básicas, muy comunes, para realizar análisis de seguridad digital son:

- ✓ Nmap (“mapeador de redes”).
- ✓ Wireshark.
- ✓ OpenVAS.
- ✓ OWA SP Zen Attack Proxy – ZAP.
- ✓ Nessus.
- ✓ Vega.
- ✓ Mesploit Framework.

También existen sistemas operativos enfocados a seguridad de digital:

- ✓ Kali Linux OS.
- ✓ Parrot OS.

Para profundizar en este punto se debe leer el siguiente contenido:

- **Nmap ("mapeador de redes"):** "Es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales**. Nmap** utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como docenas de otras características. Aunque generalmente se utiliza **Nmap** en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos." Nmap.org (2021).
- **Wireshark:** "Analizador de protocolos de red más importante y utilizado del mundo. Le permite ver lo que está sucediendo en su red a un nivel microscópico y es el estándar de facto (y a menudo de jure) en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas. El desarrollo de WireShark prospera gracias a las contribuciones voluntarias de expertos en redes de todo el mundo y es la

continuación de un proyecto iniciado por Gerald Combs en 1998.” WireShark.org (2021)

- **OpenVAS:** “Es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste del rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.

  El escáner obtiene las pruebas para detectar vulnerabilidades de un feed que tiene un largo historial y actualizaciones diarias”.OpenVas.org (2021)
- **OWASP Zen Attack Proxy – ZAP**: es un escáner de seguridad que permite descubrir vulnerabilidades en las aplicaciones web. “La Fundación OWASP ® trabaja para mejorar la seguridad del software a través de sus proyectos de software de código abierto, liderados por la comunidad, cientos de capítulos en todo el mundo, decenas de miles de miembros y organizando conferencias locales y globales.” Owasp.org (2021)
- **Nessus:** “Es un escáner de vulnerabilidades con el cual se pueden realizar evaluaciones de seguridad profundas y de alta velocidad, tiene soporte a través de Tenable Community, y es ideal para educadores, estudiantes e individuos que inician sus carreras en ciberseguridad”. Basado en tenable.com (2021)
- **Vega:** "Es un escáner de seguridad web gratuito y de código abierto y una plataforma de prueba de seguridad web para probar la seguridad de las aplicaciones web. Vega puede ayudarlo a encontrar y validar SQL Injection, Cross-Site Scripting (XSS), información confidencial divulgada

inadvertidamente y otras vulnerabilidades. Está escrito en Java, basado en GUI y se ejecuta en Linux, OS X y Windows." Subgraph.com/vega (2021)

- **Metasploit Framework :**"El Metasploit Framework (MSF) es mucho más que una simple colección de exploits, sino que también es una base sólida que se puede aprovechar y personalizar fácilmente para satisfacer sus necesidades. Esto le permite concentrarse en su entorno objetivo único y no tener que reinventar la rueda. Consideramos que MSF es una de las herramientas de auditoría de seguridad más útiles disponibles gratuitamente para los profesionales de la seguridad en la actualidad. Desde una amplia gama de exploits de grado comercial y un amplio entorno de desarrollo de exploits, hasta herramientas de recopilación de información de red y complementos de vulnerabilidad web. Metasploit Framework proporciona un entorno de trabajo realmente impresionante." Offensive-Security.com (2021)

También existen sistemas operativos enfocados a seguridad digital, los cuales contienen una serie de herramientas de seguridad informática para las revisiones de ciberseguridad, entre los más populares están:

- **Kali Linux OS**

Es un sistema operativo GNU/Linux basado en Debian. Contiene preconfiguradas, diversas herramientas software para realizar pruebas de seguridad. "La plataforma de pruebas de penetración de Kali Linux contiene una amplia gama de

herramientas y utilidades. Desde la recopilación de información hasta los informes finales, Kali Linux permite a los profesionales de la seguridad y de TI evaluar la seguridad de sus sistemas". Kali.org (2021)

- **Parrot OS**

  Es una distribución GNU / Linux basada en Debian y diseñada pensando en la seguridad y la privacidad. Incluye un laboratorio portátil completo para todo tipo de operaciones de seguridad cibernética, desde pentesting hasta análisis forense digital e ingeniería inversa, pero también incluye todo lo necesario para desarrollar su propio software o mantener sus datos seguros- Parrotsec.org (2021).

5. Inventario de activos y evaluación de impacto de riesgos

El inicio del análisis de riesgos en ciberseguridad, una vez que se haya apropiado una metodología de riesgos, es empezar por el inventario de activos de información y, a partir de allí, valorar la importancia de los mismos, los riesgos asociados, controles y determinación del riesgo inherente y residual, concluyendo con el establecimiento de un plan de tratamiento de riesgos.

Inventario de activos y evaluación de impacto de riesgos

Estudie este punto, a profundidad, en el Anexo. Analice, uno a uno, los elementos conceptuales y operativos que allí se muestran y, de ser posible, tome nota en su libreta personal de apuntes.

6. Riesgos

En términos generales, el riesgo se asocia a una “Contingencia o proximidad de un daño". RAE (2021). Cuando se realiza un análisis de riesgos de ciberseguridad, lo que se pretende es encontrar cuál es la proximidad o probabilidad de que los riesgos, amenazas y vulnerabilidades, afecten los activos de información y generen un impacto adverso en la organización.

Se debe visualizar atentamente y con sentido crítico el vídeo que se comparte a continuación. En este se podrá ampliar los conocimientos en lo relacionado con los riesgos de la ciberseguridad:

Video 3. Análisis, valoración de riesgos y controles de ciberseguridad: riesgos

Enlace de reproducción del video

Síntesis del video: Video 3. Análisis, valoración de riesgos y controles de ciberseguridad: riesgos
El proceso de análisis de los riesgos de la ciberseguridad en una organización, busca determinar cuán posibles y probables son las afectaciones que sufrirían los activos de información y la organización misma, si los riesgos, vulnerabilidades y amenazas llegan a materializarse. **Inventario de amenazas** Las vulnerabilidades y amenazas son los principales elementos que componen los riesgos de ciberseguridad de los sistemas de información, por eso es importante realizar un inventario de amenazas. Para realizar el inventario de amenazas se deben considerar: • Las amenazas identificadas. • La descripción de dichas amenazas. • El tipo de amenaza (si es una amenaza natural, industrial, un error no intencionado o un ataque intencionado). • El tipo de activo de información que afectaría. • Las dimensiones o principios de seguridad de la información que serían afectados (Confidencialidad, Integridad, disponibilidad u otras). Elementos vulnerables asociados: ✓ Hardware

- ✓ Software
- ✓ La Red
- ✓ El Personal
- ✓ Las Instalaciones físicas
- ✓ Controles de seguridad informática
- ✓ Controles para la seguridad física
- ✓ Antivirus
- ✓ Entre otros…

Catálogo de Riesgo

Con base en el inventario de amenazas se puede construir el **catálogo de riesgos**, a partir de la identificación de los principios de la seguridad de la información que son afectados por la amenaza y el tipo de amenaza.

Así entonces, el riesgo es igual a la probabilidad, por el valor del activo, por el impacto general de las dimensiones de impacto.

Riesgo R = Probabilidad (P) X Activo (A) X Impacto (I)

En el proceso, es muy importante también, **determinar la causa del riesgo**. La causa del riesgo se construye con la amenaza que aprovecha o genera una vulnerabilidad en los principales elementos vulnerables asociados.

Entonces,

Causa = Amenaza + principales elementos vulnerables asociados

Registro del catálogo de riesgos

El catálogo de riesgos, al ser un instrumento de registro, deberá contener tanto los riesgos identificados como las causas que los generan, lo cual facilita establecer las acciones o intervenciones que mitigarían o eliminarían los riesgos, amenazas o vulnerabilidades.

7. Valoración

La valoración de riesgos es un proceso que inicia con la valuación de los activos de información, luego pasa por la valoración de la probabilidad de ocurrencia de riesgos asociados a los activos y termina con la valoración del impacto.

En términos generales el riesgo es igual a la probabilidad por impacto; **Riesgo = Probabilidad x Impacto.** Pero en ciberseguridad el impacto está determinado por el valor del activo de información por el impacto general de las dimensiones de impacto organizacionales.

7.1. Riesgo inherente

Consiste en el riesgo valorado antes de que se le haya aplicado un tratamiento o controles para su mitigación. También es denominado riesgo potencial.

Sobre el riesgo inherente, se debe tener en cuenta:

Proceso temprano

Es importante que se determine este tipo de riesgo inicialmente para poder luego aplicar los controles de ciberseguridad y determinar el riesgo residual, logrando entender que controles son necesarios de fortalecer, cambiar o implementar.

Escala de evaluación

La escala de evaluación de riesgos puede ser determinada como cada organización crea conveniente, y es importante que determine los niveles de aceptación y tratamiento de riesgos.

Tabla 4. Referencia de severidad del riesgo

N.	Valor	Descripción	Acción	Límite inferior	Límite superior
1	Severo	El nivel del riesgo es Inadmisible o severo, por lo que es necesario implementar controles en la Organización para mitigar, evitar o compartir el riesgo y llevar el mismo a niveles aceptables.	Evitar / Reducir / Transferir	70	125
2	Moderado	El nivel de riesgo es Tolerable o moderado de acuerdo a los criterios de aceptación de la Organización. Los riesgos en	Aceptar / Monitorear	20	69

N.	Valor	Descripción	Acción	Límite inferior	Límite superior
		esté nivel deben ser monitoreados para identificar oportunamente los cambios en su valoración.			
3	Leve	El nivel de riesgo es Aceptable y se encuentra controlado en la Organización o el mismo es insignificante. Los riesgos en esté nivel se deben revisar periódicamente.	Aceptar	1	19

7.2. Evaluación de controles de seguridad

La evaluación de controles es un aspecto importante dentro del análisis de riesgos, para ello se deben inventariar los controles existentes y realizar la evaluación, conforme a los detalles de referencia.

El inventario de controles se debe realizar siguiendo la siguiente estructura:

- ✓ Número de control.
- ✓ Nombre del control.
- ✓ Descripción del control.
- ✓ Asignación del control.
- ✓ Tipo de control: preventivo, correctivo.
- ✓ Naturaleza del control.
- ✓ Frecuencia.

- ✓ Evidencia/Documentación.
- ✓ Funcionalidad.

Se debe conocer la referencia de evaluación de controles que el siguiente recurso tiene. Allí mismo, se debe ampliar el conocimiento en la determinación de diseños de control y ejecución de los controles. ¡Adelante!

1. Para comenzar, analice y comprenda esta tabla de referencia para la evaluación de controles.

Asignación	Valor	Tipo	Valor	Naturaleza	Valor	Frecuencia	Valor	Documentación	Valor	Evidencia/ Soporte	Funcionalidad	Valor
Asignado	30%	Preventivo	10%	Automático	20%	Adecuada	10%	Documentado	10%	Actas de comité o actas de reuniones	Adecuada	20%
No Asignado	0%	Detectivo	7%	Desarrollo de TI	7%	Inadecuada	0%	No documentado	0%	Archivos digitales	Inadecuada	0%
- -	- -	Correctivo	5%	Manual	5%	- -	- -	- -	- -	Correos corporativos	- -	- -
- -	- -	- -	0%	- -	0%	- -	- -	- -	- -	Check list	- -	- -
- -	- -	- -	- -	- -	- -	- -	- -	- -	- -	Formatos	- -	- -
- -	- -	- -	- -	- -	- -	- -	- -	- -	- -	Informes de gestión	- -	- -

Asignación	Valor	Tipo	Valor	Naturaleza	Valor	Frecuencia	Valor	Documentación	Valor	Evidencia/ Soporte	Funcionalidad	Valor
- -	- -	- -	- -	- -	- -	- -	- -	- -	- -	Políticas organizacionales - procedimientos	- -	- -
- -	- -	- -	- -	- -	- -	- -	- -	- -	- -	Registros financieros	- -	- -
- -	- -	- -	- -	- -	- -	- -	- -	- -	- -	Registros administrativos	- -	- -
- -	- -	- -	- -	- -	- -	- -	- -	- -	- -	Registros operativos	- -	- -
- -	- -	- -	- -	- -	- -	- -	- -	- -	- -	Registros digitales	- -	- -

2. Una vez inventariados y evaluados los controles, se debe determinar el diseño del control, la ejecución, la solidez individual, la importancia del control y la solidez del conjunto del control.
3. El Diseño del control es la sumatoria de la Asignación del control con el Tipo de control (Preventivo, Correctivo) + la Naturaleza del control, la Frecuencia y la Funcionalidad.
4. Analice, ahora, esta tabla referencia para determinar la ejecución, solidez e importancia de controles.

N,	Ejecución	Descripción	Valor	Solidez	Valor	Límite inferior	Límite inferior	Importancia	Descripción	Valor
1	Fuerte	Control que se ejecuta cada vez que se desarrolla la actividad.	5	Fuerte	5	16	25	Muy Importante	Si el control garantiza cero errores.	5
2	Moderado	Control que se aplica en momentos determinados.	3	Moderado	3	9	15	Importante	Si el control garantiza un buen desempeño.	3
3	Débil	Control que se efectúa cuando se requiere.	1	Débil	1	1	5	Poco Importante	Si lo que aporta el control no es significativo.	1

5. La ejecución del control se determina manualmente, mientras que la Solidez individual será igual al diseño del control por la ejecución del control.
6. Así entonces: solidez individual del control
7. Si= Diseño del control X Ejecución del control

7.3. La importancia del control

La Importancia del control se determina manualmente; habiéndola determinado es más sencillo determinar la solidez del conjunto de control, que es el resultado que ayudará a determinar si el control puede, o no, disminuir un riesgo. La solidez del conjunto de control es igual a la solidez individual del control más la Importancia, sobre tres (3).

Solidez del conjunto de control, Sc = (solidez individual del control + Importancia) / 3

Se debe tener muy presente los aspectos que se muestran en el siguiente recurso, sobre la importancia del control y la solidez del conjunto de controles; no olvidar la toma de nota sobre ellos:

- **División sobre tres:** se divide sobre tres (3) teniendo en cuenta los valores de referencia que se han utilizado.
- **Coherencia con la realidad**: es importante que en cada método de valoración o medición establecido en la organización se determine que, el mismo, sea coherente y pueda representar lo mejor posible la realidad.
- **Referencia:** esta es la referencia para determinar la solidez del conjunto de controles:

Tabla 5. Referencia para determinarla solidez del conjunto de controles

Calificación	ES	Valor	Límite inferior	Límite superior	Disminución de la probabilidad e/o impacto
Fuerte	>=	3.3	3.3	5	2
Moderado	>= Y <	2.5 – 3.2	3.2	2.5	3.2
Débil	<	2.5	0	2.4	0

Nota. Tomado de Modelo MSPI. MinTic. (2016).

- Solidez del conjunto de controles: cuando se aplican varios controles en el tratamiento de un riesgo, el promedio de la Solidez del conjunto de control de los controles aplicados, determina la Solidez del conjunto de controles para la disminución de la probabilidad e/o impacto.

- **Aplicación de controles a riesgos**

Tabla 6. Referencia de aplicación de controles a riesgos

Riesgo	Sc. Control 1	Sc. Control 2	Sc. Control 3	Sc. Control n	Promedio Sc. controles	Disminuye probabilidad	Disminuye impacto
Riesgo 1	NA	3.3	2.7	...	3	1	1
Riesgo 2	1	3.3	2.7	...	2.33	0	0

7.4. Riesgo residual

El riesgo residual, consiste en el riesgo repercutido o resultante, después de que se aplican controles o medidas para la reducción de los mismos.

Se debe prestar atención a los siguientes aspectos a tener en cuenta en lo referente al riesgo residual:

- ✓ **Su determinación**

  La determinación del riesgo residual se realiza a partir de que un control disminuye la probabilidad o impacto de un riesgo.

- ✓ **¿Qué debe haberse hecho?**

Para determinar riesgos, es importante que se haya realizado un adecuado inventario, evaluación de controles y aplicación de los mismos a los riesgos del catálogo de riesgos, según corresponda.

✓ **Acciones de tratamiento**

Una vez que se tengan los riesgos residuales se deben aplicar actividades de tratamiento para aquellos que como resultado, dieron críticos, altos o muy altos, según se considere.

8. Matriz de riesgos

La matriz de riesgos se construye a partir de las evaluaciones de activos, probabilidad de riesgos, el impacto, controles y el riesgo residual. La matriz de riesgos permite tener la trazabilidad necesaria del resultado de análisis de un riesgo o de un activo de información.

La matriz debe contener un registro y valoración de:

- Activos de información.
- Riesgos; (Amenazas, principios afectados por amenazas, elementos vulnerables).
- Probabilidad de riesgos.
- Dimensiones de Impactos organizacionales.
- Cálculo del Riesgo inherente.
- Controles y aplicación de controles al catálogo de riesgos.

- Cálculo del riesgo residual.

8.1. Diligenciamiento de la matriz de riesgos

La matriz de riesgos se convierte en instrumento clave para lograr que la organización gestiones y determinar con la mayor objetividad, todos y cada uno de los riesgos relevantes y no relevantes, que afectarían o no, y en qué medida, la ciberseguridad y la seguridad de la información, así como también la seguridad general de la infraestructura, el talento humano, las redes de servicios, los procesos, etc.

Diligenciar la matriz de riesgos, es una acción sencilla que implica analizar los procesos, funciones y tareas que, en la organización, desarrollan tanto sus colaboradores como, incluso, los activos mismos de información. Visualice y analice la referencia de matriz de riesgos que le presentamos, ver la siguiente tabla:

Tabla 7. Referencia matriz de riesgos

	Activo y riesgo inherente	Activo y riesgo inherente	Activo y riesgo inherente	Activo y riesgo inherente	Elementos vulnerables asociados	Elementos vulnerables asociados	Elementos vulnerables asociados	Elementos vulnerables asociados	Elementos vulnerables asociados
Activo	Valor activo	Probabilidad Total	Impacto General	Riesgo Inherente	Controles	Nueva probabilidad	Nuevo impacto	Riesgo residual	Nivel de severidad
Servidor Web	5	4	5	**100**	X	3	4	**60**	**Moderado**
Información Documental	5	4	3	**60**	X	4	2	**40**	**Moderado**

	Activo y riesgo inherente	Activo y riesgo inherente	Activo y riesgo inherente	Activo y riesgo inherente	Elementos vulnerables asociados	Elementos vulnerables asociados	Elementos vulnerables asociados	Elementos vulnerables asociados	Elementos vulnerables asociados
…	…	…	…	…	…	…	…	…	…

8.2. Plan de tratamiento de riesgos

Una vez se tenga la matriz de riesgos se debe desarrollar un plan de tratamiento de riesgos PTR. En ciberseguridad, consiste en una serie de actividades a desarrollar, en función de riesgos de ciberseguridad no aceptables, severos o críticos, resultantes del proceso de análisis de riesgos; tales actividades buscan fortalecer, corregir o implementar controles de ciberseguridad para la reducción de riesgos asociados a los activos de información.

El plan de tratamiento de riesgos se debe construir considerando los siguientes aspectos:

- Activo de Información con riesgos críticos.
- Riesgos residuales asociados.
- Causas de riesgo asociadas.
- Controles asociados a los riesgos.

Tipo de tratamiento; mitigar o reducir el riesgo, evitar el riesgo, compartir o transferir el riesgo.

- Actividades a realizar.
- Responsable.

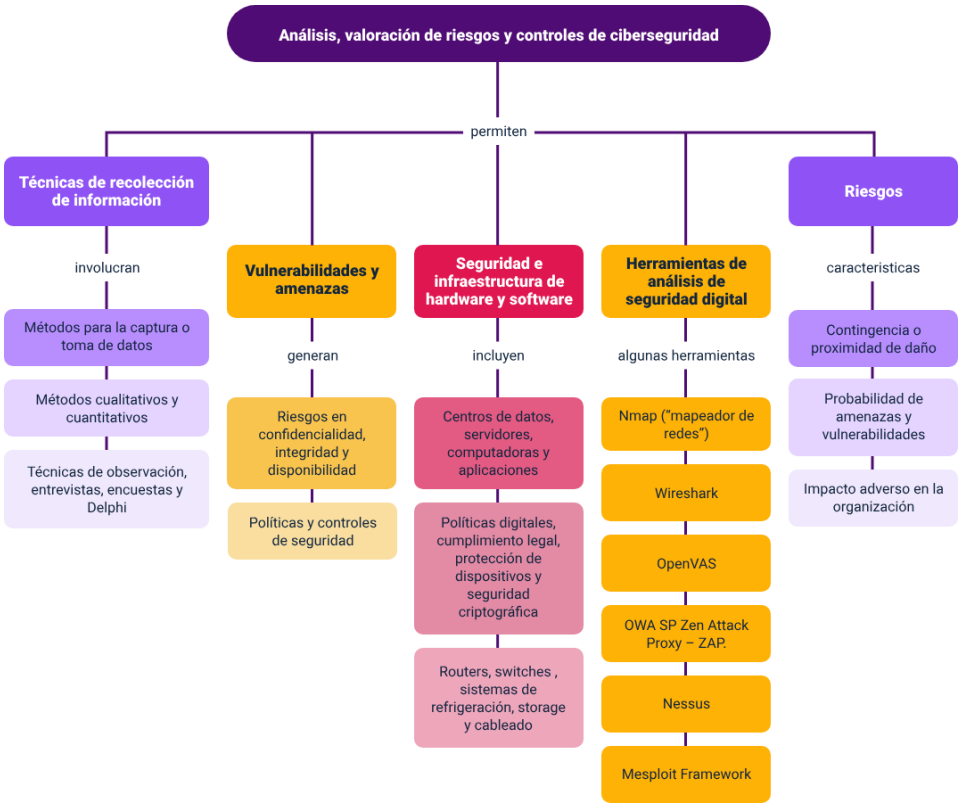
- Prioridad.
- Fecha de Implementación de las actividades.
- Observaciones.

Una vez se haya realizado el Plan de Tratamiento de Riesgos se debe comunicar a las partes interesadas, principalmente a los responsables de los activos de información y se debe dejar un registro de aceptación del plan de tratamiento de riesgos.

El **PTR**, plan de tratamiento de riesgos, debe ser revisado periódicamente para determinar la conformidad, según las fechas de implementación de las actividades.

Síntesis

En resumen, el componente formativo ofrece una visión integral y práctica de la ciberseguridad, desde la recolección de datos hasta la valoración y gestión de riesgos, proporcionando herramientas y técnicas esenciales para garantizar la seguridad digital en las organizaciones. A continuación, se presenta un mapa conceptual que resume la información de este proceso.



Glosario

Activo de información: componente el cual almacena, trata, muestra o transporta datos e información, pudiendo ser físicos o digitales, por ejemplo, una base de datos, software, sistemas de información, papel, discos duros, personas, procesos, etc.

Amenaza: se define como toda aquella acción o serie de acciones que aprovechan las vulnerabilidades para romper la seguridad de los sistemas.

Autenticidad: 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].

***Cloud Computing*:** la computación en la nube se refiere a la utilización de soluciones *hardware* y *software* dispuestos a través de internet para la implementación de soluciones informáticas.

Confidencialidad de la información: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE 71504:2008].

Control o salvaguarda: medida de protección o control para contrarrestar amenazas.

Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

***Hardware*:** componentes tecnológicos de carácter físico que soportan el *software*.

Infraestructura TI: la infraestructura tecnológica consiste en los componentes de *hardware* y *software* requeridos para gestionar y operar entornos tecnológicos que pueden ser implementados en instalaciones de la organización o en sistemas en la nube, *Cloud Computing*.

Integridad de los datos: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].

Riesgo: contingencia o proximidad de un daño. RAE (2021).

***Software*:** componente intangible compuesto por un sistema, servicios, programas y/o aplicaciones. Es un mecanismo para realizar instrucciones a los componentes de *hardware* en un sistema informático, como a los microprocesadores.

Trazabilidad: propiedad o Característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

Vulnerabilidad: en informática, se define como una debilidad o fallo de seguridad que se presenta en un sistema de información, que puede estar compuesto por *software*, *hardware* y otros componentes y servicios tecnológicos, generando riesgos de seguridad de la información.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
	Tenable. (2021). Tenable for education, Instructor / Student guide	Página web	https://static.tenable.com/marketing/whitepapers/Guide-Tenable-for-Education.pdf
	Owasp. (2021). OWASP ZAP 2.9. Getting Started Guide.	Página web	https://www.zaproxy.org/pdf/ZAPGettingStartedGuide-2.9.pdf
	SUBGRAPH. (2021). About Vega.	Página web	https://subgraph.com/vega/documentation/about-vega/index.en.html

Referencias bibliográficas

Chaves, E. (2009). Manual metodológico para la recolección de Información. http://funes.uniandes.edu.co/21233/1/Chaves2009Manual.pdf

Gallardo, Y. & Moreno A. (1999). Serie aprender a investigar. Módulo recolección de la información. http://www.unilibrebaq.edu.co/unilibrebaq/images/CEUL/mod3recoleccioninform.pdf

International Business Machines Corporation. (2021). ¿Qué es infraestructura de TI? IBM.

https://www.ibm.com/co-es/topics/infrastructure

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Catálogo de Elementos. https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Ministerio de Tecnologías de la Información y Comunicaciones. (2012). Guía de gestión de riesgos. Seguridad y privacidad de la información.

https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Nmap Security. (2021). Guía de referencia de Nmap. NMAP. https://nmap.org/man/es/index.html#man-description

OpenVas by Greenbone. (2021). OpenVAS: escáner de evaluación de vulnerabilidades abiertas. OPENVAS.

https://www.openvas.org/

Peña, O. (2020). ¿Para qué sirven las técnicas de recolección de información? POLIVERSO.

https://www.poli.edu.co/blog/poliverso/tecnicas-de-recoleccion-de-informacion

Real Academia Española. (2021). Riesgo. RAE

https://dle.rae.es/riesgo

WireShark.org. (2021). Analizador de protocolos de red. WIRESHARK. https://www.wireshark.org/

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Líder del Ecosistema	Dirección General
Nombre completo	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Nombre completo	Diseñador Instruccional	Centro - Regional
Nombre completo	Experto Temático	Centro - Regional
Nombre completo	Asesor Metodológico	Centro - Regional
Nombre completo	Corrector de Estilo	Centro - Regional
Nombre completo	Diseñador de Contenidos Digitales	Centro - Regional
Nombre completo	Desarrollador Full-Stack	Centro - Regional
Nombre completo	Locución	Centro - Regional
Nombre completo	Storyboard e Ilustración	Centro - Regional
Nombre completo	Animador y Productor Audiovisual	Centro - Regional
Nombre completo	Validación de Recursos Educativos Digitales	Centro - Regional
Nombre completo	Evaluador para Contenidos Inclusivos y Accesibles	Centro - Regional