**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Tecnólogo en Implementación y operación de la Ciberseguridad |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501108 - Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501108-02 - Realizar el análisis y valoración de riesgos de ciberseguridad acorde con los métodos definidos. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 02 |
| NOMBRE DEL COMPONENTE FORMATIVO | 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. |
| PALABRAS CLAVE | Activo de información, amenazas, controles, metodología de análisis, riesgo. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | Servicios |
| IDIOMA | Español |

1. **Tabla de contenidos**

**Introducción**

**1.** **Técnicas de recolección de información**

1.1. Técnicas de recolección más usuales

1.2. Características de las técnicas de recolección

**2.** **Vulnerabilidades y amenazas**

2.1. Valoración de amenazas y vulnerabilidades

2.2. Tratamiento de riesgos

**3.** **Seguridad e infraestructura de *hardware* y *software***

3.1. Infraestructura de *hardware* y *software*

3.2. Componentes de infraestructura y seguridad

3.3. Interconexiones de redes y seguridad perimetral

**4.** **Herramientas de análisis de seguridad digital**

**5. Inventario de activos y evaluación de impacto de riesgos**

**6.** **Riesgos**

**7. Valoración**

7.1. Riesgo inherente

7.2. Evaluación de controles de seguridad

7.3. La importancia del control

7.4. Riesgo residual

**8. Matriz de riesgos**

8.1. Diligenciamiento de la matriz de riesgos

8.2. Plan de tratamiento de riesgos

1. **DESARROLLO DE CONTENIDOS**

**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.



<https://cdn.pixabay.com/photo/2018/10/06/16/10/security-3728124_960_720.jpg>

Para comenzar, se debe revisar el siguiente recurso:



DI\_CF2\_Introduccion

**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.



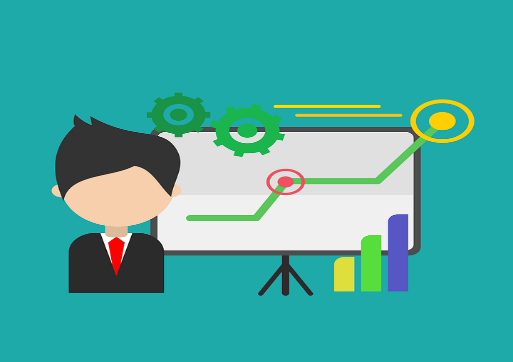
<https://cdn.pixabay.com/photo/2016/05/03/00/07/analytics-1368293_960_720.png>

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:

DI\_CF2\_1-1\_Conceptos

**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.



<https://cdn.pixabay.com/photo/2020/04/04/04/22/analysis-5000776_960_720.png>

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

DI\_CF4\_1-1\_TecnicasRecoleccionMasUsuales

**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.



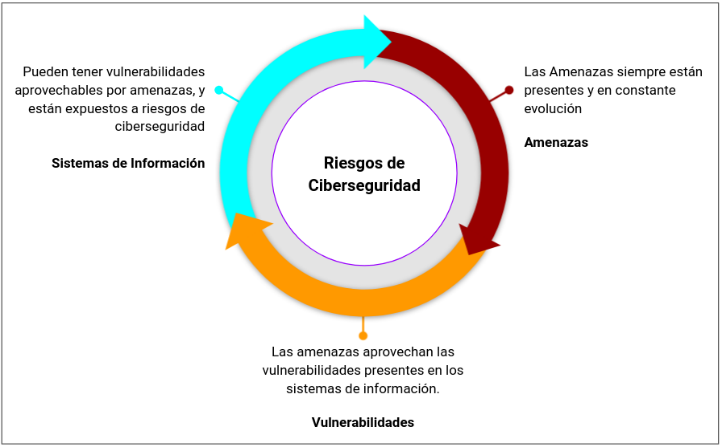
<https://cdn.pixabay.com/photo/2016/12/22/13/35/analytics-1925495_960_720.png>

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

DI\_CF2\_1-2\_CaracgeristicasTecnicasRecoleccion

**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.



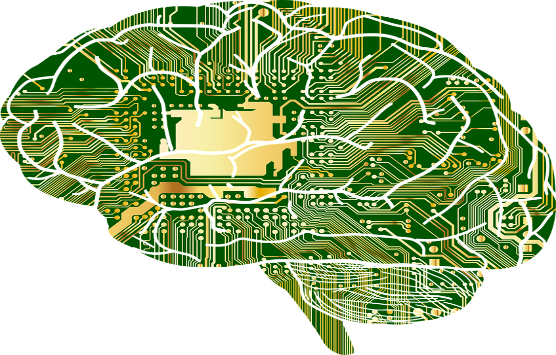
<https://www.incibe.es/sites/default/files/contenidos/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian/riesgo.png>

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

DI\_CF2\_VulnerabilidadesYAmenzas

**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.



<https://cdn.pixabay.com/photo/2016/10/18/19/40/anatomy-1751201_960_720.png>

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

* **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).

* **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).

* **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 2 | | Riesgo 3 | | Riesgo n | |
| 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.



<https://cdn.pixabay.com/photo/2019/09/01/06/20/cyber-4444448_960_720.jpg>

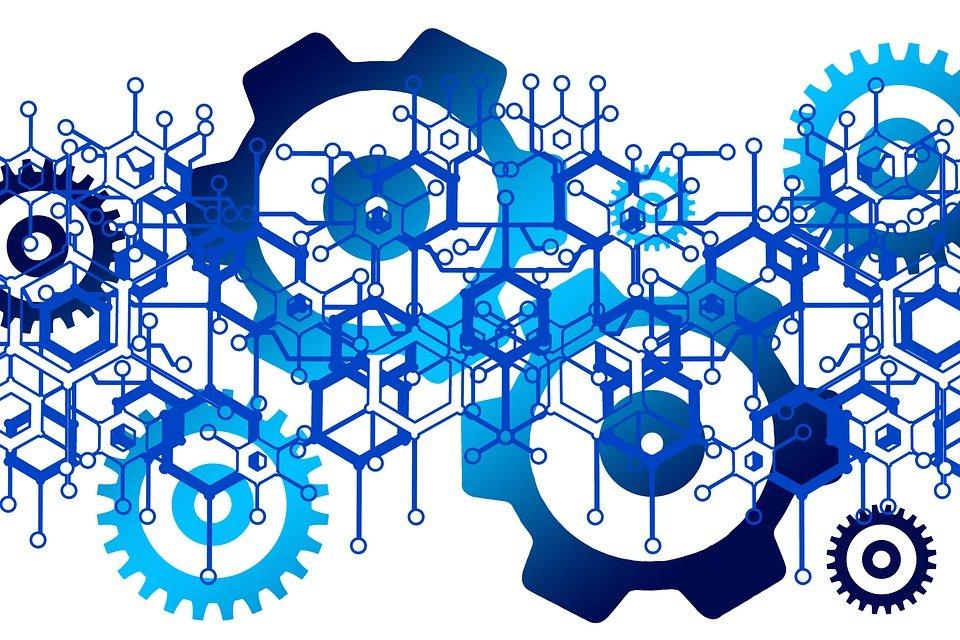
Las características que se deben considerar para realizar un plan de tratamiento de riesgos son:

* 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.



**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).*



<https://cdn.pixabay.com/photo/2021/08/28/06/14/blockchain-6580140_960_720.jpg>

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.*



<https://media.istockphoto.com/photos/stock-exchange-market-concept-businesswoman-hand-trader-press-digital-picture-id1276312812?s=612x612>

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!

DI\_CF2\_3-1\_InfraestructuraHardwareYSoftware

**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.



<https://cdn.pixabay.com/photo/2016/04/16/10/42/binary-1332816_960_720.jpg>

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

DI\_CF2\_3-2\_ComponentesInfraestructuraYSeguridad

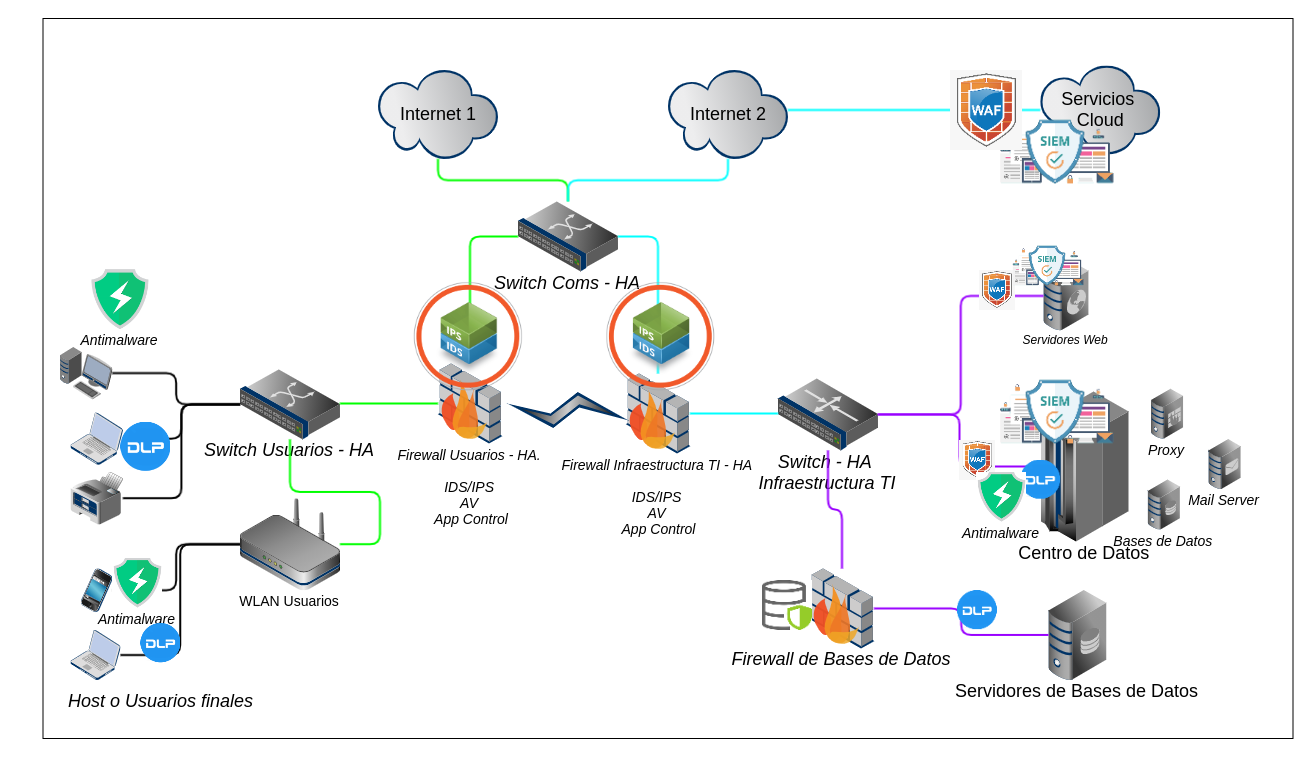
**3.3. Interconexiones de redes y seguridad perimetral**

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:

**Figura 1**

*Interconexión de redes y seguridad perimetral*





**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.*



<https://cdn.pixabay.com/photo/2015/08/27/09/22/banner-909710_960_720.jpg>

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 explorar el siguiente recurso didáctico:

DI\_CF2\_4\_HerramientasAnalisisSeguridadDigital

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**

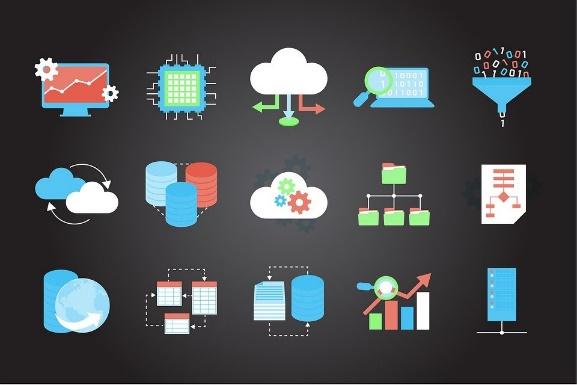
Es un sistema operativo GNU/Linux basado en Debian. Contiene preconfiguradas, diversas herramientas *software* para realizar pruebas de seguridad. "La plataforma de pruebas de penetración de Kali Linux contiene una amplia gama de herramientas y utilidades. Desde la recopilación de información hasta los 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.



<https://cdn.pixabay.com/photo/2018/05/16/20/07/technology-3406895_960_720.jpg>

Estudie este punto, a profundidad, en el **Anexo\_1\_ActivosInformacionEImpactoDeRiesgos**. 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.



<https://cdn.pixabay.com/photo/2018/01/12/16/17/graph-3078546_960_720.png>

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:

DI\_CF4\_6\_Riesgos

**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.

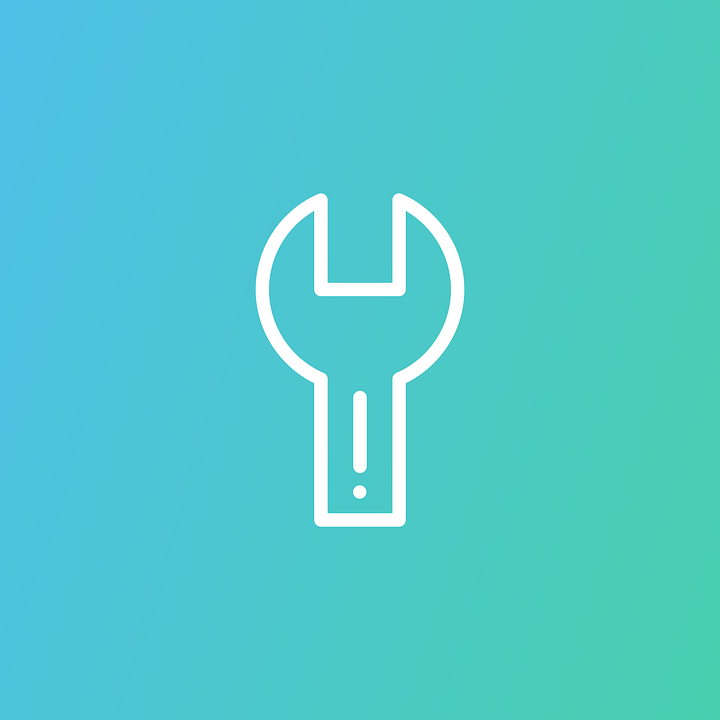


<https://cdn.pixabay.com/photo/2017/02/16/11/59/horizontal-2071302_960_720.jpg>

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.



<https://cdn.pixabay.com/photo/2017/03/21/02/00/tool-2160921_960_720.png>

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.

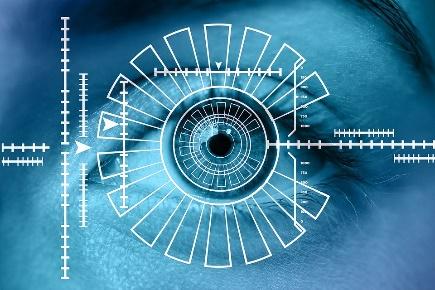
**Escala de evaluación**

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.



* 1. **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.



<https://cdn.pixabay.com/photo/2017/09/21/08/56/eye-2771174_960_720.jpg>

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**!

DI\_CF2\_7-2\_EvaluacionControlesSeguridad

* 1. **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).

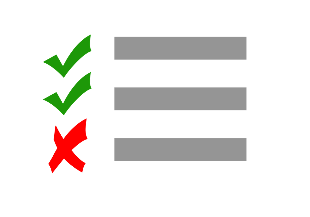
Solidez del conjunto de control, Sc = (solidez individual del control + Importancia) / 3

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:

DI\_CF2\_7-3\_LaImportanciaDelControl

* 1. **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.



<https://cdn.pixabay.com/photo/2016/05/19/09/32/checklist-1402461_960_720.png>

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.

1. **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.



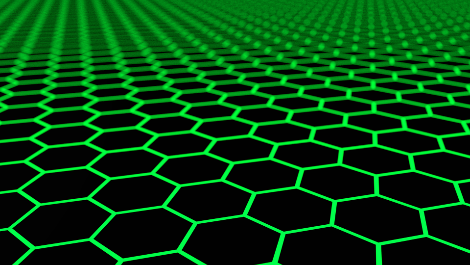
<https://cdn.pixabay.com/photo/2015/11/06/13/12/matrix-1027571_960_720.jpg>

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.



<https://cdn.pixabay.com/photo/2016/05/24/14/42/green-1412466_960_720.png>

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 tabla 12.

**Tabla 12**

*Referencia matriz de riesgos*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Activo | ACTIVO Y RIESGO INHERENTE | | | | CONTROLES Y RIESGO RESIDUAL | | | | |
| *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 |
| ... | … | …. | ... | ... | ... |  |  |  | ... |

* 1. **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.



<https://cdn.pixabay.com/photo/2021/08/17/06/32/business-6552135_960_720.jpg>

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.

1. **SINTESÍS**

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.

Diagrama

Descripción generada automáticamente

1. **Actividades didácticas (opcionales si son sugeridas)**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Explorando la fortaleza digital: herramientas fundamentales de análisis de seguridad. |
| Objetivo de la actividad | Establecer un marco conceptual que me permita el uso y la aplicación efectiva de herramientas de análisis de seguridad digital, *incluyendo Nmap, Wireshark, OWASP ZAP, Nessus, Vega y Metasploit Framework*, con el fin de identificar vulnerabilidades, analizar patrones de tráfico y realizar evaluaciones de seguridad detalladas. |
| Tipo de actividad sugerida | Relacionar términos |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexos/CF02\_Formato\_5\_actividad\_didactica\_relacionar\_terminos\_DI\_2023 |

1. **Material complementario**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tema** | **Referencia APA del Material** | **Tipo de material   (Video, capítulo de libro, artículo, otro)** | **Enlace del Recurso o   Archivo del documento o material** |
| 3. Seguridad e Infraestructura de *hardware* y *software* | Tenable. (2021).  *Tenable for education, Instructor / Student guide* | Página web | <https://static.tenable.com/marketing/whitepapers/Guide-Tenable-for-Education.pdf> |
| 3.3. Interconexiones de redes y seguridad perimetral | Owasp. (2021).  *OWASP ZAP 2.9. Getting Started Guide* | Página web | <https://www.zaproxy.org/pdf/ZAPGettingStartedGuide-2.9.pdf> |
| 4. Herramientas de análisis de seguridad digital | SUBGRAPH. (2021). *About Vega* | Página web | <https://subgraph.com/vega/documentation/about-vega/index.en.html> |
| 4. Herramientas de análisis de seguridad digital | Tenable. (2021).  *Tenable for education, Instructor / Student guide* | Página web | <https://static.tenable.com/marketing/whitepapers/Guide-Tenable-for-Education.pdf> |

1. **Glosario**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| 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. |

1. **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/>

1. **Control del documento**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Joaquín Patiño Cerón | Experto Temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Agosto 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Tolima - Centro Agropecuario La Granja | Septiembre 2021 |
| Andrés Felipe Velandia Espitia | Revisor Metodológico y Pedagógico | Regional Distrito Capital – Centro de Diseño y Metrología | Septiembre 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor Pedagógico | Regional Santander – Centro Industrial del Diseño y la Manufactura | Septiembre 2021 |
| Jhon Jairo Rodríguez Pérez | Diseñador y evaluador instruccional | Regional Distrito Capital - Centro para la Industria de la Comunicación Gráfica. | Septiembre 2021 |

1. **CONTROL DE CAMBIOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| Autor (es) |  |  |  |  |  |