**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 | 220501108-01. Establecer métodos de análisis y valoración de riesgos de ciberseguridad, de acuerdo con estándares internacionales y normatividad nacional. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | CF01 |
| NOMBRE DEL COMPONENTE FORMATIVO | Fundamentos de seguridad digital y análisis de riesgos |
| BREVE DESCRIPCIÓN | Con el estudio de este componente, el aprendiz profundizará en los fundamentos necesarios para diagnosticar el estado actual de la ciberseguridad en una organización, adoptando métodos de análisis y valoración de riesgos, como elementos fundamentales para definir un plan de tratamiento adecuado. |
| PALABRAS CLAVE | Activo de información, Ciberseguridad, Estándar, Metodología, Riesgo |

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

1. **TABLA DE CONTENIDOS:**

**Introducción**

**1. Fundamentos de Redes y *Networking***

1.1. Conceptos

1.2. Características

1.3. Tipos de redes

1.4. Modelo OSI

1.5. Protocolo TPC/IP

1.6. Protocolos IPv4 e IPv6

1.7. Enrutamiento IP

**2. Normatividad y estándares: ciberseguridad**

**3. Normatividad y estándares: seguridad de la información**

**4. Marco legal**

**5. Marco Jurídico**

**6. Tipificación de delitos informáticos en Colombia**

**7. Activos de Información**

7.1. Características de los activos de información

7.2. Tipos de activos de información

7.3. Técnicas de valoración de activos

**8. Amenazas y Vulnerabilidades**

8.1. Características y tipos de amenazas y vulnerabilidades

8.2. Vulnerabilidades del sistema

8.3. Amenazas de ataques de denegación de servicio

8.4. Vulnerabilidades producidas por contraseñas

8.5. Vulnerabilidades producidas por usuarios

8.6. Otras amenazas informáticas

**9. Riesgos**

9.1. Niveles de riesgo

9.2. Características, impacto y análisis de riesgo

**10. *Ethical Hacking***

10.1. Objetivos del *ethical hacking*

10.2. Tipos de pruebas de penetración

1. **DESARROLLO DE CONTENIDOS:**

**Introducción**



Por medio del diagnóstico de la seguridad digital, se logra establecer el estado actual de la ciberseguridad de una organización. Gracias a dicho diagnóstico, es posible también, adoptar estándares de seguridad y metodologías para el análisis de riesgos informáticos, disponibles en el mercado. He ahí la importancia de su reconocimiento y elección, de acuerdo a los requerimientos de la organización sobre la cual se está generando un modelo de seguridad.

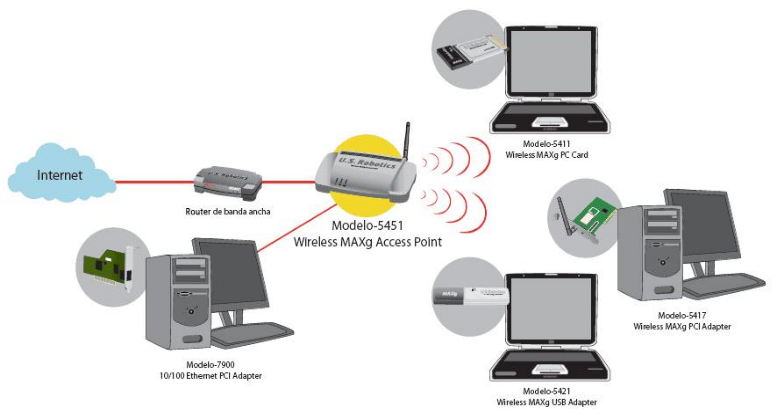


<https://cdn.pixabay.com/photo/2018/07/14/11/33/earth-3537401_960_720.jpg>

Esto quiere decir que existen varios métodos, metodologías y estándares, con los cuales se pueden hacer análisis de riesgos. En este componente formativo se conceptualizará al respecto y, en esa tarea, se explicarán las metodologías para el análisis de riesgos y los estándares adecuados con sus respectivos controles para la seguridad.

**1. Fundamentos de Redes y *Networking***

Para dar comienzo a este recorrido formativo por los **fundamentos de seguridad digital y los análisis de riesgos**, presentamos algunos conceptos claves que orientarán la asimilación de los contenidos. Preste toda su atención y disponibilidad para su estudio.



<https://estecnoinformatic.com/c-informatica-basica/elementos-de-una-red-funcion-principal-grafica-y-mas/>

**1.1. Conceptos**

Una red de computadoras es un conjunto de ordenadores y otros dispositivos que se conectan entre sí, tanto de manera alámbrica, es decir por cables, o inalámbricas ósea *wifi*, para intercambiar información y compartir recursos.



<https://cdn.pixabay.com/photo/2016/04/04/14/12/monitor-1307227_960_720.jpg>

**Información para cada propósito**

Las redes informáticas tienen la capacidad de dar la información para cada propósito de negocios, entretenimiento e investigación.

**Conexión unificada**

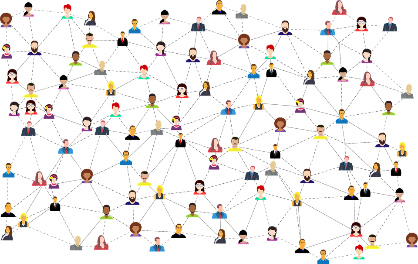
También da la posibilidad de adecuar una única conexión a internet en varios ordenadores.

**Intercambio de información y dispositivos**

La red informática tiene la habilidad de compartir impresora y otros periféricos, además de enviar y recibir mensajes y pasar archivos a otros ordenadores sin necesitar de un cd, memoria usb u otro elemento.

**1.2. Características**

En este punto, las características hacen referencia a los elementos que componen una red: *Host, Switch, Router, Servidor, Firewall*, etc.



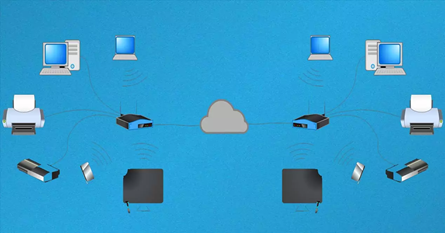
<https://cdn.pixabay.com/photo/2018/11/29/21/51/social-media-3846597_960_720.png>

En el siguiente recurso, le presentamos las topologías de red más importantes; conozca y asimile cada una de ellas:

DI\_CF1\_1-2\_Caractaristicas

**1.3. Tipos de redes**

Las redes informáticas o de ordenadores se pueden clasificar de varias formas o tipos diferentes. Aquí le mostramos los tipos de redes más importantes y destacados y que, además, son los más usados:



<https://www.redeszone.net/app/uploads-redeszone.net/2020/05/redes-lan.jpg>

* + LAN (red de área local): su finalidad se relaciona con la unión de varios ordenadores y dispositivos conectados a un servidor.
  + WLAN (red de área local inalámbrica): una WLAN tiene la misma función que una LAN, pero las conexiones se realizan de forma inalámbrica.

* + WAN (red de área amplia): son las redes de mayor alcance, como lo es la red global de redes, Internet.
  + MAN (red de área metropolitana): las MAN suelen ser más grandes que las LAN, tienen como función, conectar distintas áreas alejadas entre sí. Son redes de tamaño intermedio.
  + PAN (red de área personal): una PAN sirve a una persona. Se utiliza generalmente para uso personal o individual cuando se requiere, por ejemplo, en la oficina o trabajo.
  + SAN (red de área de almacenamiento): Pueden gestionar una gran cantidad de tráfico. Es una red que forma parte de empresas que trabajan con servidores y quieren mantener un buen rendimiento.
  + CAN (red de área de campus): se puede inferir que se encuentra entre una LAN y una MAN. No es tan pequeña como una LAN, pero tampoco es tan grande como una MAN.
  + VPN (red privada virtual): Una VPN realiza un canal cifrado que mantiene la identidad y las credenciales de acceso de un usuario, así como cualquier dato transferido.

**1.4. Modelo OSI**

Teniendo en cuenta que, en general, los conjuntos de protocolos de red se estructuran en capas, la Organización Internacional para la Estandarización (ISO) ha implementado el modelo de referencia de Interconexión de Sistemas Abiertos (OSI) que maneja capas estructuradas. El modelo OSI es el modelo de la interconexión de sistemas abiertos. El modelo OSI está conformado por siete capas para las actividades de red y cada capa tiene asociados uno o más protocolos.



<https://cdn.pixabay.com/photo/2015/05/15/21/36/finger-769300_960_720.jpg>

En la siguiente tabla, entérese de cuáles son esas capas y las especificidades de cada una de ellas:

**Tabla 1**

*Modelo de referencia de Interconexión de Sistemas Abiertos.*

|  |  |  |
| --- | --- | --- |
| Nº de capa | Nombre de capa | Descripción |
| 7 | Aplicación | Hace referencia a cada uno de los servicios y/o las aplicaciones de comunicación estándar, que pueden ser manipulados o utilizados por cualquier usuario. |
| 6 | Presentación | La presentación corrobora que la información sea transferida hasta el sistema receptor de manera comprensible para el sistema. |
| 5 | Sesión | Dirige las conexiones y terminaciones entre los sistemas que cooperan. |
| 4 | Transporte | Manda la transferencia de datos. Así mismo, asegura que los datos recibidos sean idénticos a los transmitidos. |
| 3 | Red | Dispone las direcciones de datos y la transferencia entre redes. |
| 2 | Vínculo de datos | Dirige la transferencia de datos en el medio de red. |
| 1 | Física | Da a conocer las características del hardware de red. |

Nota: Tomada de la Guía de administración del sistema: servicios IP (2010).

**1.5. Protocolo TPC/IP**

TCP/IP son las siglas de las siguientes palabras: *Transmission Control Protocol/Internet Protocol* (Protocolo de control de transmisión/Protocolo de Internet). Los protocolos TCP/IP son un conjunto de reglas para formatos de mensajes y procedimientos, que permiten que el *hardware* y los *softwares* de aplicación, intercambien información.



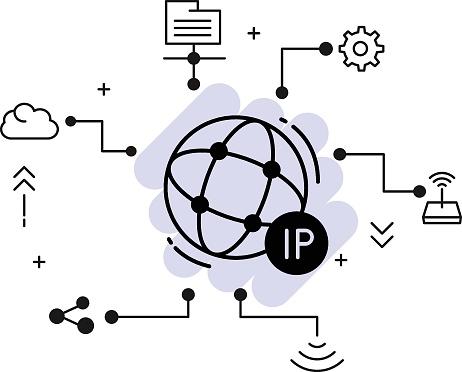
<https://cdn.pixabay.com/photo/2019/03/18/06/46/cyber-4062449_960_720.jpg>

Despliegue el recurso que se muestra a continuación para tener un primer acercamiento conceptual a los protocolos TCP / IP y descubra cómo estos se disponen en capas.

DI\_CF1\_1-5\_ProtocolosTCP-IP

**1.6. Protocolos IPv4 e IPv6**

El *Internet Protocol Version* 4 (IPv4), conocido como el sistema de identificación que usa Internet para enviar información entre los dispositivos, maneja direcciones de 32 bits con hasta 12 caracteres, en cuatro bloques de 3 caracteres, cada bloque. El (DNS) los convierte en nombres de dominio como *1and1.es.* ajustando todos los dígitos.



<https://media.istockphoto.com/vectors/internet-protocol-address-concept-sticky-dynamic-ip-vector-glyph-icon-vector-id1328876600?b=1&k=6&m=1328876600&s=170667a&w=0&h=9RoPZGHFDrNn44MMCGVyIv1HPxtYlNqpkaA_OMyXr6o>=

Por otra parte, está el *Internet Protocol Version* 6 (IPv6); su espacio de direcciones es de 128-bits. Este protocolo aumenta el tamaño de la dirección IP de 32 bits a 128 bits para así resistir más niveles en la jerarquía de direccionamiento y un número mayor de nodos direccionables. El diseño del protocolo, suma muchos beneficios en seguridad: una mayor capacidad de transmisión, manejo de calidad de servicio y mejora la facilidad de administración.

Los siguientes puntos son los beneficios que representa un proceso de transición de **IPv4** al **IPv6**, que son importantes tener presentes, al momento de adoptar el nuevo protocolo:

DI\_CF1\_1-6\_IPv4-IPv6

**1.7. Enrutamiento IP**

Acceder a la comunicación e interconectividad de redes, a través de paquetes IP enviados desde un origen a un destino, aprovechando la tecnología con la que cuenta cada *router*, permite diversas configuraciones y protocolos. Algunas de sus utilidades son, entre otras, poder hallar redes remotas, conservar la información de enrutamiento actualizada, elegir el mejor camino hacia las redes de destino, poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible.



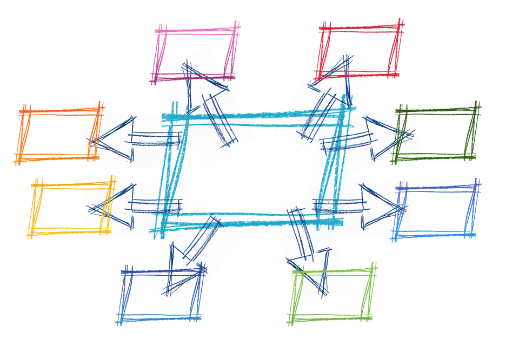
<https://cdn.pixabay.com/photo/2018/03/10/09/45/businessman-3213659_960_720.jpg>

Descubra los tipos de enrutamiento IP que se presentan en el siguiente recurso. Conozca, además, sus ventajas y desventajas. Le sugerimos tomar nota atenta de los aspectos más importantes. ¡**Adelante**!

**2. Normatividad y estándares: ciberseguridad**

La normalización o **estandarización**, elabora una serie de especificaciones técnicas – NORMAS – que son adoptadas de manera voluntaria.



<https://cdn.pixabay.com/photo/2017/01/18/08/20/network-1989138_960_720.png>

La legislación (Artículo 8 de la Ley 21/1992 de Industria) define la norma como la “especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba un Organismo reconocido, a nivel nacional o internacional, por su actividad normativa”.

Para profundizar y afianzar en aspectos importantes relativos a normatividad y estándares, visite el recurso que se presenta a continuación. Haga un estudio consciente de todos los elementos que allí se muestran.

DI\_CF1\_2\_NormatividadEstandaresCiberseguridad

**3. Normatividad y estándares: seguridad de la información**

De la misma manera que en los procesos de seguridad de la información y ciberseguridad, es importante en la gestión de riesgos de la seguridad de la información, utilizar los lineamientos de las siguientes normas y estándares:



<https://cdn.pixabay.com/photo/2018/09/11/14/42/dsgvo-3669706_960_720.jpg>

DI\_CF1\_3\_NormatividadSeguridadInformacion

**4. Marco legal**

El CONPES 3701, es la base de la legislación relacionada con esta temática. La Comisión Nacional Digital y de Información Estatal, fue creada a través del **Decreto 32** de **2013** del Ministerio de Tecnologías de la Información y las Comunicaciones. Petición que tiene el objeto 34 de encargarse de la coordinación y orientación superior del desarrollo de funciones y servicios públicos que tienen que ver con el manejo de la información pública, el uso de infraestructura tecnológica de la información, y la utilidad de la información en el Estado colombiano.



<https://st2.depositphotos.com/1996555/5506/i/600/depositphotos_55064783-stock-photo-colombia-law-concept.jpg>

(Departamento Nacional de Planeación, 2011).

Visite el recurso que le presentamos a continuación y conozca más y mejor sobre el marco legal en procesos de ciberseguridad y seguridad de la información. Una vez más le insistimos en tomar nota de los aspectos más relevantes.

DI\_CF1\_4\_MarcoLegal

**5.Marco Jurídico**

Para prevenir y combatir la delincuencia informática, se ha avanzado a nivel global en la aplicación de campañas, técnicas, programas, normas y leyes que responden, en cada país o región, a los eventos más concurrentes relativos a ese fenómeno.



<https://www.vendesfacil.com/wp-content/uploads/2018/06/delitos-inform%C3%A1ticos.jpg>

El gobierno colombiano ha establecido la siguiente base jurídica para enfrentar los delitos informáticos:

* Comercio electrónico ley 527/1999
* Violación ilícita de comunicaciones ley 599/2000
* Uso de medios tecnológicos ley 962/2005
* Notificación electrónica ley 1150/2007
* Protección de la información ley 1273/2009
* Agencia del espectro electromagnético ley 1341/2009
* Seguridad en redes. Resolución 2258/2009
* Seguridad y calidad navegable de información. Circular. 052/2009

**6. Tipificación de delitos informáticos en Colombia.**

En la actualidad, el amplio uso de las tecnologías y la cantidad en aumento de usuarios en las redes y los sistemas, ha favorecido la implantación de los delitos informáticos, es decir, todas aquellas acciones gravemente engañosas y de fraude que pueden cometerse en los ámbitos digitales y *on line*.



<https://cdn.pixabay.com/photo/2019/01/09/10/24/information-technology-3923009_960_720.jpg>

Según la Ley 1273 de 2009, se ajustaron los delitos informáticos en Colombia en los siguientes términos:

* Acceso abusivo a un sistema informático (modificado del Código Penal).
* Obstaculización ilegítima del sistema informático o red de telecomunicación.
* Interceptación de datos informáticos.
* Daño informático; uso de software malicioso.
* Hurto por medios informáticos y semejantes.
* Violación de datos personales.
* Suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos.

**7. Activos de Información:**

Los activos de información relacionados con la seguridad de la información, hacen referencia a cualquier información o dispositivo que tenga que ver con el tratamiento de ésta y que sea de valor para la organización.



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

Los activos de información cuentan con un sistema de clasificación, el cual se enfoca en las propiedades de confidencialidad, integridad y disponibilidad, como elementos para el tratamiento de los datos. Además, evalúa el impacto que tendría, en caso de no cumplir alguno de estos fundamentos.

Los activos de información se clasifican, generalmente, en activos de prioridad alta, media y baja; de esta manera se establece cuáles se deben tratar con prelación.

**Alta**

Se determina cuando la clasificación es de dos, en todas las propiedades (confidencialidad, integridad, disponibilidad).

**Media**

Se ubica en esta posición si la clasificación de la información de una de las propiedades es alta o nivel medio.

**Baja**

Se considera baja cuando la clasificación de la información en todas sus propiedades es baja.

**7.1. Características de los activos de información**

Los activos de información presentan características diferentes según el estado, la materia, los niveles de confidencialidad, la integridad y la disponibilidad.



<https://cdn.pixabay.com/photo/2016/03/09/10/37/light-1246043_960_720.jpg>

Estas son las características más representativas, y a tener en cuenta, de los activos de información:



**7.2. Tipos de activos de información**

Se relacionan cinco grandes tipos de activos de información, de la siguiente manera:

**Seguridad**

Todo el ambiente del Sistema de Gestión de Seguridad de la Información según la **ISO 27001**, que contenga a los activos y que es necesario que garanticen los diferentes niveles de seguridad.



<https://cdn.pixabay.com/photo/2020/05/18/16/17/social-media-5187243_960_720.png>

**El sistema mismo**

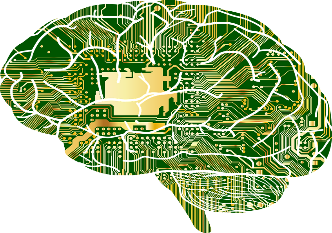
El propio sistema de información es considerado como uno de los tipos de activos.



<https://cdn.pixabay.com/photo/2018/03/21/07/16/learning-3245793_960_720.jpg>

**Información generada**

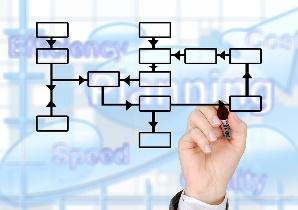
Toda la información que se ha generado por la aplicación del Sistema de Gestión de Seguridad de la Información.



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

**Funciones empresariales u organizacionales**

Todas las funciones de una organización, con las que se pueden demostrar las diferentes exigencias del Sistema de Gestión de Seguridad de la Información y, además, genera los objetivos deseados.



<https://cdn.pixabay.com/photo/2014/11/04/08/07/mark-516277_960_720.jpg>

**Métodos o sistemas de valoración de riesgos**

Es otro tipo de activos, aquellos que pueden realizar un método de evaluación de riesgos para facilitar la inclusión de cualquier otro activo.



<https://cdn.pixabay.com/photo/2016/11/30/12/09/question-mark-1872634_960_720.jpg>

**7.3. Técnicas de valoración de activos**

La técnica que será utilizada para valorar se encuentra apoyada en los activos que se encuentran en los inventarios; tienen una parte de activos que están vinculados con el entorno y otra parte que se encuentran clasificados en otros inventarios. Los activos que pueden estar, o no, en los inventarios, por lo general se encuentran en las aplicaciones que existen en la obtención de información. Otro tipo de activos no pueden estar en el inventario, ya que en este caso dejarían de tener valor.



<https://cdn.pixabay.com/photo/2018/05/08/08/44/artificial-intelligence-3382507_960_720.jpg>

Si se realizan técnicas de valoración del estado de seguridad de los activos que se tienen en cuenta para estimar todos los valores, se utilizan según los cuatro subestados que se mencionan a continuación (A-C-I-D):

**Subestado Autentificación**

Baja.

Normal.

Alta.

Crítica.

**Subestado Confidencialidad**

Libre.

Restringida.

Protegida.

Confidencial.

**Subestado Integridad**

Bajo.

Normal.

Alto.

Crítico.

**Subestado Disponibilidad**

Menos de una hora.

Hasta un día laborable.

Hasta una semana laborable.

Hasta un mes laborable.

**8. Amenazas y vulnerabilidades**

Las vulnerabilidades y amenazas informáticas se relacionan con los riesgos que se pueden generar para los sistemas y la información de una organización. Este fenómeno es cada vez más frecuente ya que, en la actualidad, existe una alta dependencia digital y de los servicios TI.



<https://cdn.pixabay.com/photo/2017/10/24/07/12/hacker-2883632_960_720.jpg>

En el siguiente recurso, le presentamos algunas definiciones claves, que le favorecerán la asimilación y conceptualización en lo referente a amenazas y vulnerabilidades informáticas.

DI\_CF1\_8\_AmenazasYVulnerabilidades

**8.1. Características y tipos de amenazas y vulnerabilidades**

En términos informáticos y organizacionales, tanto las amenazas y las vulnerabilidades son propias de los sistemas de una compañía y esto la hace siempre susceptible. Las amenazas y vulnerabilidades atentan contra la seguridad de un sistema de información y exponen la seguridad de la información frente a los ataques que comprenden la integridad, disponibilidad o confidencialidad de la misma.



<https://cdn.pixabay.com/photo/2016/11/07/12/08/cyber-security-1805632_960_720.png>

### El principal tipo de amenaza que tiene el sistema de información de cualquier organización es la Amenaza de *Malware*; los programas maliciosos o inseguros son una de las mayores ciberamenazas a las que se enfrentan las organizaciones. Dentro del *malware* se encuentran las siguientes amenazas:

**Los virus**

Los virus informáticos son los que se instalan en un dispositivo con el fin de proporcionar dificultades en su funcionamiento.

**Gusanos**

Este es uno de los *malware* más comunes que infectan los equipos y sistemas de una empresa.

**Troyanos**

Los troyanos son instalados en un equipo y pasan desapercibidos para el usuario.

***Ransomware***

Su función es encriptar toda la información de la organización, interrumpiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información.

***Keyloggers***

Son instalados a través de troyanos y su función es robar datos de acceso a plataformas web, sitios bancarios y similares.

### **8.2. Vulnerabilidades del sistema**

De manera frecuente, tanto los sistemas informáticos como las aplicaciones informáticas, suelen tener algún tipo de errores en su diseño, o en su estructura; incluso es altamente frecuente que presenten fallas en su código, dando comienzo o cabida a cualquier vulnerabilidad.



<https://cdn.pixabay.com/photo/2016/07/23/10/51/binary-1536651_960_720.jpg>

Siempre que exista un error, incluso si este no es notorio o grande, será posible generar algún tipo de amenaza en los sistemas y sobre la información de las organizaciones, favoreciendo así ataques tanto externos como internos.

A continuación, le contamos dónde suelen presentarse las principales vulnerabilidades:

* + Fallas de configuración.
  + Fallas en la gestión de recursos.
  + Fallas en los sistemas de validación.
  + Errores que generan el acceso a directorios.
  + Errores en la gestión y asignación de permisos.

### **8.3. Amenazas de ataques de denegación de servicio**

Cuando se habla de ataque por denegación de servicio distribuido, (***DDoS***) se logra establecer que este, se genera en el momento en que el servidor recibe demasiadas solicitudes o peticiones de acceso.



<https://cdn.pixabay.com/photo/2018/05/14/15/53/cyber-security-3400555_960_720.jpg>

Esta situación de sobredemanda en solicitudes al servidor es la razón por la cual se presenta un colapso del sistema, provocando que el servidor se abata o que alcance un funcionamiento incorrecto, por ejemplo, acceso lento o rebote de mensajes de errores.

**8.4. Vulnerabilidades producidas por contraseñas**

No tener contraseñas seguras, que sean difíciles de descifrar, genera vulnerabilidades en los sistemas, ya que facilita el robo, la modificación o eliminación de información, cambiar configuraciones si disponen de los privilegios apropiados o, incluso, apagar equipos.



<https://cdn.pixabay.com/photo/2016/02/16/16/57/login-1203603_960_720.png>

La creación de contraseñas seguras es una de las claves para incrementar el nivel de ciberseguridad de las empresas.

### **8.5. Vulnerabilidades producidas por usuarios**

Los ataques informáticos suelen tener como causa principal, el uso no adecuado de los usuarios. Cuando se conceden privilegios o permisos que no son usados pertinentemente, se pueden generar accesos de los usuarios a opciones, tanto de configuración como de administración, para los cuales no se encuentran preparados.



<https://cdn.pixabay.com/photo/2017/10/30/18/44/hacking-2903156_960_720.jpg>

Visite el recurso que se muestra a continuación, en él le presentamos algunos aspectos que debe tener en cuenta, relacionados con las vulnerabilidades producidas por usuarios:

DI\_CF1\_8-5\_VulenerabilidadesProducidasPorUsuarios

**8.6. Otras amenazas informáticas**

Se conocen otras amenazas informáticas que afectan a las empresas como los ataques por Inyección **SQL**, que afectan a servidores de bases de datos empresariales, red de equipos *zombies*, ataques MITM (*man in the middle*), etc.



<https://cdn.pixabay.com/photo/2015/02/08/16/19/keyboard-628703_960_720.jpg>

Estas son algunas particularidades que usted debe conocer y tener en cuenta, en lo referente a amenazas informáticas diversas:

**Ataques innovadores, ciberseguridad dinámica**

La ciberdelincuencia no para y, por lo general, buscan nuevas formas de atacar, infectar y robar información de las organizaciones; es por esto que la ciberseguridad debe ser una actividad flexible y dinámica que se adapte a las nuevas amenazas.

**Eliminación constante de vulnerabilidades**

Las vulnerabilidades exponen a las organizaciones frente a las amenazas informáticas. Entonces, es importante enfocarse en eliminar vulnerabilidades, como una de las principales acciones de la ciberseguridad para reducir las amenazas informáticas.

**Desde el exterior**

Son múltiples los tipos y maneras de vulnerabilidades y/o amenazas informáticas. La mayoría de estas amenazas y/o vulnerabilidades, tienen origen en el exterior, como por ejemplo el *malware* o los ataques DDoS.

**Desde el interior**

Otras amenazas o vulnerabilidades tienen su origen al interior de los sistemas y suelen ser ocasionadas por los mismos usuarios o colaboradores de las empresas u organizaciones: entre los más comunes están los robos, los accesos con privilegios incorrectos o, simplemente, errores humanos.

**9. Riesgos**

Se conoce como riesgo a toda posibilidad de sufrir una afectación por causa de factores externos o internos. El riesgo es un peligro latente que puede o no materializarse. En el orden informático y de ciberseguridad, los riesgos no son distintos. Contemplan las vulnerabilidades y las amenazas y pueden ser controlados, tratados, mitigados, prevenidos y, en algunos casos, eliminados.



<https://cdn.pixabay.com/photo/2016/08/27/15/50/privacy-policy-1624400_960_720.jpg>

A continuación, se mencionan los tipos de riesgos de ciberseguridad más comunes; conózcalos y tome nota atenta de ellos:

* + ***Malware***

Se refiere a todos aquellos archivos que contaminan y pueden comprometer tanto la seguridad, como la utilidad y preservación del equipo.

* + ***Phishing* o usurpación de identidad**

Se hace una serie de actos fraudulentos, ya sea a través de correos o mensajes de entidades reconocidas para generar confianza.

* + ***Criptomining***

Es un delito en el cual se dirigen ataques a las cuentas, sea un usuario o empresa.

* + **Ataques DDoS**

El término de DDoS se debe a su nombre en inglés (*Distributed Denial of Service*) la cual tiene el objetivo de ejecutar un ataque de denegación de servicio distribuido.

* + ***Ransomware***

Consiste en un sistema malicioso el cual restringe o prohíbe el acceso a los datos confidenciales.

* + ***Botnets***

Se trata de una amenaza para los ordenadores actuando a través de troyanos que se filtran en el mismo para así enviar información como spam.

* + **Inyección SQL**

Se aprovecha la vulnerabilidad de la validación de acceso a un sitio o aplicación, con la finalidad de infiltrarse en su base de datos para obtener información de los usuarios.

**9.1. Niveles de riesgo**

Los riesgos, suelen estar tipificados según su nivel de probabilidad, de impacto y de daño potencial. La clasificación de los riesgos en niveles, es un elemento que favorece la previsión de los mismos, el tratamiento y control que se les podría aplicar y las demás acciones de actualización y monitoreo de los sistemas de información.



<https://cdn.pixabay.com/photo/2017/10/26/11/21/ssl-2890762_960_720.jpg>

Estudie, en el siguiente recurso, los niveles en los que se clasifican los riesgos:

DI\_CF1\_9-2\_NivelesDeRiesgo

**9.2. Características, impacto y análisis de riesgos**

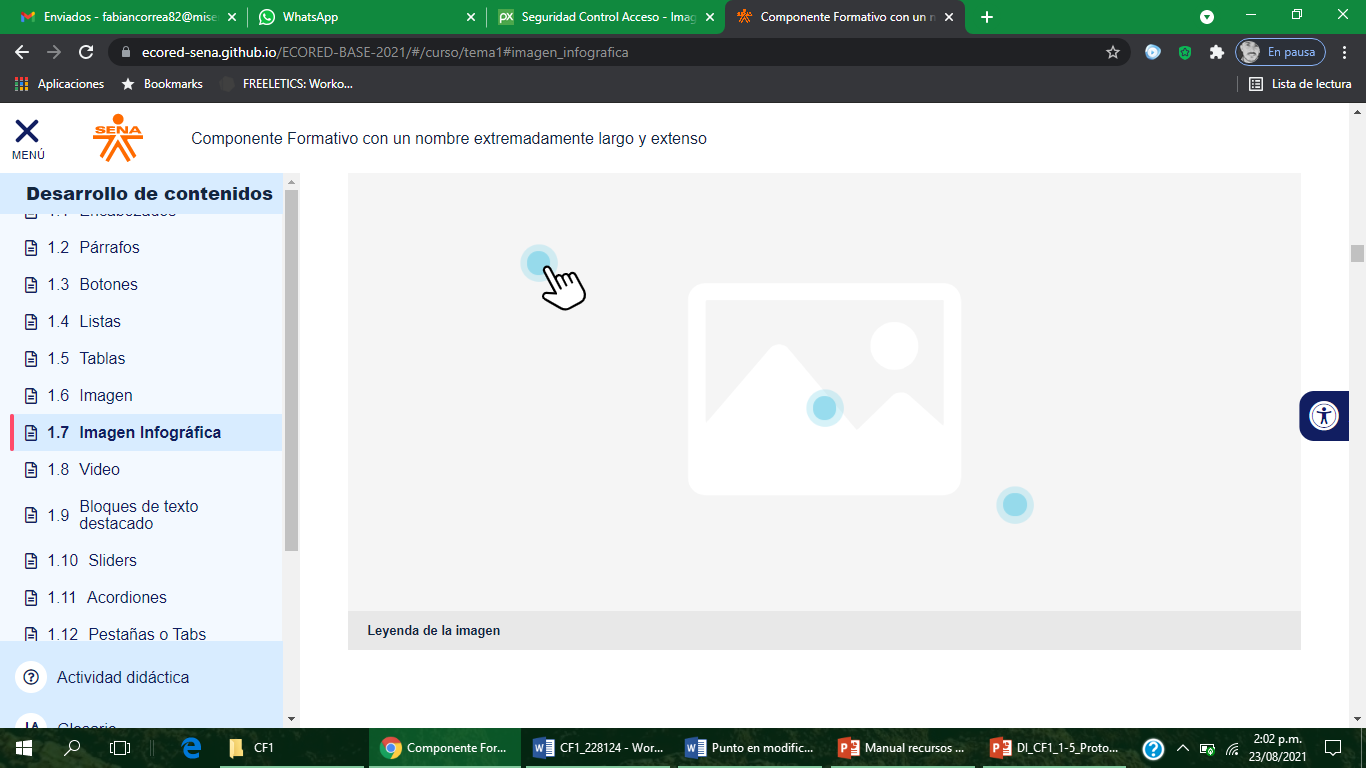
La existencia de vulnerabilidades y posibles fallas en los sistemas informáticos, facilitan que la información pueda ser empleada maliciosamente para conseguir ventajas de ella o que sea manipulada para afectar la infraestructura tecnológica, física y del entorno.



<https://cdn.pixabay.com/photo/2019/09/23/08/50/security-4497950_960_720.png>

Le mostraremos, a continuación, aspectos importantes sobre los riesgos, su impacto y probabilidad, su análisis y tratamiento. Además, algunos conceptos nuevos que le afianzarán en su saber sobre ciberseguridad.

DI\_CF1\_9-2\_CaracteristicasImpactoYAnalisisRiesgos



Para estudiar a profundidad las técnicas de tratamiento de riesgos y afianzarse en la adopción de controles de seguridad, le recomendamos hacer búsqueda de la norma **ISO / IEC 27005** y la norma **ISO 31000:2018**.

***https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es***

**10. *Ethical Hacking***

Un *Hacker* Ético es una persona que realiza pruebas de penetración con la intención de buscar y encontrar vulnerabilidades actuando de forma igual, o al menos similar, y utilizando los mismos métodos que usaría un *hacker* con intención de atacar el sistema.



<https://cdn.pixabay.com/photo/2019/10/02/14/23/privacy-policy-4521074_960_720.jpg>

Las pruebas de penetración de un hacker ético, permiten evaluar vulnerabilidades, analizar y categorizar las debilidades explotadas y proveer recomendaciones, en base a las prioridades de la organización y por último eliminar dichas vulnerabilidades.

**10.1. Objetivos del *ethical hacking***

El objetivo fundamental del *Ethical Hacking* es explorar las vulnerabilidades existentes en los sistemas, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc.



<https://cdn.pixabay.com/photo/2020/03/20/08/01/hacker-4949897_960_720.jpg>

Esta técnica logra el acceso y demuestra si un sistema es vulnerable o no. Esta información sirve para tomar medidas preventivas en contra de ataques.

**10.2. Tipos de pruebas de penetración**

Dentro del ejercicio del *ethical hacking*, existen tres tipos de pruebas de penetración: caja negra, caja blanca y caja gris.



<https://cdn.pixabay.com/photo/2020/05/24/09/51/security-5213398_960_720.jpg>

Descubra las particularidades de cada una de estos tres tipos de pruebas de penetración.

**Prueba de la caja negra**

La caja negra es cuando el *Ethical Hacker* no tiene información sobre el objetivo o la red. Esta prueba es la mejor para simular un ataque externo e ignora las amenazas internas.

**Prueba de la caja blanca**

La Prueba de caja blanca es lo opuesto a una caja negra. El *Ethical Hacker* tiene pleno conocimiento de la red, los sistemas informáticos y la infraestructura. La prueba de la caja blanca permite una prueba exhaustiva del entorno.

**Prueba de la caja gris**

La Prueba de caja gris, simula una amenaza interna. El *Ethical Hacker* recibe información parcial sobre la red y los sistemas informáticos, como configuraciones de IP, listas de correo electrónico, nombres de computadora u otra información que una persona con información privilegiada tendría de manera realista.

1. **ACTIVIDADES DIDÁCTICAS (OPCIONALES SI SON SUGERIDAS)**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad |  |
| Objetivo de la actividad |  |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) |  |

**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 |
| 9.2. Características, impacto y análisis de riesgos | ISO (2018). *Gestión del riesgo. Directrices (*ISO 31000). | Norma / Documento | <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es> |
| 2. Normatividad y estándares: ciberseguridad  3. Normatividad y estándares: seguridad de la información | ISO (2018). *Seguridad de la información, ciberseguridad y protección de la privacidad* (ISO 27005) | Norma / Documento | <https://www.iso.org/standard/75281.html> |
| 2. Normatividad y estándares: ciberseguridad  3. Normatividad y estándares: seguridad de la información | ISO (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad* (ISO 27002) | Norma / Documento | <https://www.iso.org/standard/54533.html> |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| **TÉRMINO** | **SIGNIFICADO** |
| **Activos de información** | Los activos de información relacionados con la seguridad de la información, hacen referencia a cualquier información o dispositivo que tenga que ver con el tratamiento de ésta y que sea de valor para la organización. |
| **Auditoría** | Se trata de aquella acción que consiste en emitir criterios y opiniones profesionales acerca de cualquier objeto de análisis, del cual se espera que represente de manera adecuada la realidad que pretende reflejar; también sobre si cumple o no con las condiciones y funcionalidades que se han acordado en el nivel de servicio. |
| **Auditorías internas de SGSI** | El principal objetivo de este tipo de auditoría de SGSI es investigar si existe algo que mal realizado, de manera objetiva. El auditor interno tiene que ser una persona capacitada, con su conocimiento debe poder descubrir si algo se hace mal dentro de la organización. Realizando un buen trabajo, correctivo y/o preventivo, entonces la auditoría interna de SGSI mejorará su seguridad. |
| **Ciberseguridad** | Conjunto de metodologías, medidas y controles destinados a gestionar la seguridad de la información de una organización y/o de la información en general. |
| ***Ethical Hacking*** | Es un proceso que se da al interior de las organizaciones a través del cual se exploran las vulnerabilidades existentes en los sistemas, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. |
| **Malware** | Se refiere a todos aquellos archivos que contaminan y pueden comprometer tanto la seguridad, como la utilidad y preservación del equipo. |
| **Riesgo** | Toda posibilidad de sufrir una afectación por causa de factores externos o internos. El riesgo es un peligro latente que puede o no materializarse. En el orden informático y de ciberseguridad, los riesgos no son distintos. Contemplan las vulnerabilidades y las amenazas y pueden ser controlados, tratados, mitigados, prevenidos y, en algunos casos, eliminados. |
| **Seguridad informática** | La seguridad informática es aquella rama del saber que tiene ocupación en el diseño de normas y criterios, procedimientos y métodos, técnicas y estrategias, dirigidos a lograr seguridad y confiabilidad en un sistema de información. |
| **Virus Informático** | Los virus informáticos son los que se instalan en un dispositivo con el fin de proporcionar dificultades en su funcionamiento. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

Cloud Education (2021). *Redes.* IBM. <https://www.ibm.com/co-es/cloud/learn/networking-a-complete-guide#toc-trminos-y--ZhqcZz4r>

Corporation and/or its affiliates (2010). *Modelo de referencia OSI.* ORACLE. <https://docs.oracle.com/cd/E19957-01/820-2981/ipov-8/index.html>

Ministerio de Hacienda y Administraciones Públicas (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* <https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf>

Ministerio de Tecnologías de la Información y las Comunicaciones (2017*). Guía de transición IPv4 a IPv6 para Colombia* <https://www.mintic.gov.co/portal/715/articles-162301_guia_transicion_ipv4_ipv6.pdf>

Organización de Estados Americanos (2019). *Ciberseguridad marco NIST. Un abordaje integral de la ciberseguridad.* <https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf>

Organización Internacional de Normalización (ISO 2013). *Seguridad de la información, ciberseguridad y protección de la privacidad* (ISO 27001). <https://www.iso.org/standard/54534.html>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Pablo Cesar Pardo Ortiz | Experto Temático | Cauca - Centro de Teleinformática y Producción Industrial | 21/08/2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Centro agropecuario La Granja, Regional Tolima | Agosto 2021 |
| Carolina Coca Salazar | Revisora metodológica y pedagógica | Regional Distrito Capital- Centro de Diseño y metrología | Agosto 2021 |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

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