Análisis y valoración de riesgos de ciberseguridad

Breve descripción:

Con 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.

Julio 2023

Grupo de Ejecución de la Formación Virtual

Tabla de contenido

Introducción

En este componente se abordarán los conceptos y fundamentos de las tecnologías de información y la seguridad de la información, reconociendo la normatividad, marcos y estándares para una adecuada gestión de riesgos de ciberseguridad y la tipificación de delitos informáticos en el contexto colombiano.

Por lo anterior, a través del siguiente video se presentan las temáticas que se abordarán en el componente formativo, destacando la importancia en los entornos empresariales, de esta manera se invita al aprendiz a disponerse para el proceso de aprendizaje.

Video 1. Análisis y valoración de riesgos de ciberseguridad.

Enlace de reproducción del video

Síntesis del video: Análisis y valoración de riesgos de ciberseguridad.
Análisis y valoración de riesgos de ciberseguridad. En la actualidad, las empresas cuentan con gran parte de la información de forma digitalizada o en la nube. Por lo cual se hace necesario gestionar los riesgos y controles para la protección de la integridad, confidencialidad y disponibilidad de este activo tan valioso. Así, los conceptos clave para valorar y clasificar los activos de información son: primero, reconocer la normatividad, el marco legal y jurídico; segundo, estándares de seguridad de la información y ciberseguridad, tipificando los delitos informáticos en el contexto colombiano; y tercero, diagnosticar el estado actual en una organización, adoptando métodos de análisis y valoración de riesgos como elementos fundamentales para definir un plan de tratamiento adecuado, de acuerdo con los requerimientos de la organización y sobre la cual se pueda generar un modelo de seguridad.

1. Fundamentos de redes y “networking”

La virtualización de muchas actividades ha transformado las bases de la sociedad y es comúnmente conocida como sociedad de la información y del conocimiento, que radica su fundamento en utilizar dispositivos digitales para las tareas diarias tales como comprar, vender, realizar operaciones financieras, entre otras, a través de un solo clic.

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 o sea “Wifi”, para intercambiar información y compartir recursos.

- **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.

A continuación, le presentamos las topologías de red más importantes; conozca y asimile cada una de ellas:

- **Punto a punto**. Cuando se habla de la topología, se está haciendo referencia al enlace constante entre dos puntos finales. Esta topología, denominada punto a punto conmutado, es básicamente el modo más tradicional de la telefonía básica. El valor que tiene una red permanente de punto a punto, está relacionado con el proceso de comunicación directo y sin obstáculos entre los puntos finales. El valor de una conexión punto-a-punto a demanda, es proporcional al número de pares posibles de abonados y se ha denominado como la ley de "Metcalfe".
- **Topología de bus.** Cuando se hace referencia a la topología de bus, hay que tener sabido que todos los equipos están conectados a un circuito común. Allí, toda la información que sea enviada desde un equipo hasta otro, viajará de manera directa o indirecta, mientras exista un controlador que enrute los datos al destino indicado. La información será procesada por el cable en ambas direcciones y lo hará a una velocidad aproximada de 10/100 Mbps y tendrá en sus dos extremos una resistencia (terminador). Es posible conectar al bus una buena cantidad de computadores o equipos y, si alguno de los computadores llega a fallar, la comunicación se podrá mantener, pero, en cambio, si la falla se presenta en el bus, entonces no sucederá lo mismo. Existen varios tipos de cableado, entre los que se puede encontrar el cableado coaxial, el par trenzado o la denominada fibra óptica. En una topología de bus, cada uno de los equipos o computadores está conectado a un segmento común de cable de red.
- **La topología en estrella.** Esta topología reduce la posibilidad de que la red falle, conectando todos los computadores a un nodo central. Cuando se pone a una red basada en la topología estrella, este concentrador central

vuelve a enviar todas las transmisiones recibidas de cualquier computador periférico a todos los computadores periféricos de la red; algunas veces, incluso, al computador que lo envió. Todos los computadores o equipos periféricos se pueden comunicar con los demás recibiendo del computador central solamente. Una falla en la línea de conexión de cualquier computador con el computador central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de los sistemas permanecería intacto.

- **Topología en anillo**. En la topología en anillo, cuando el nodo central es pasivo, el nodo origen ha de tener la capacidad de tolerar un eco de su transmisión. Una red, en estrella activa, tiene un nodo central activo que, generalmente, cuenta con los medios necesarios para prevenir problemas afines al eco.

  La red en anillo, es básicamente una topología de red a través de la cual, cada estación tiene una única conexión de entrada y otra de salida. Cada estación cuenta con un receptor y un transmisor que tiene como función ser traductor, es decir, que pasa la señal a la estación siguiente. A través de un token, conocido también como testigo. La comunicación, en este tipo de red, es permitida; es así como se logran evitar las probables pérdidas de información por colisiones.

- **La topología en árbol.** A la topología en árbol también se le conoce como topología jerárquica y se le puede definir como la colección de redes, en estrella, que tiene un orden jerárquico. Esta tipología de árbol cuenta con nodos periféricos individuales que requieren tanto transmitir como hacer recepción, únicamente, de otro nodo; y no se requiere, que actúen como

repetidores o regeneradores. La función del nodo central es posible distribuirla, de manera contraria a como se hace en las redes en estrella. Como en las redes en estrella convencionales, los nodos individuales podrían permanecer aislados de la red por un fallo puntual en la ruta de conexión del nodo.

- **Topología en malla.** La topología de red mallada tiene como finalidad tener conectado cada nodo, a todos los nodos. De esta manera es posible dirigir los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está totalmente conectada, no puede existir ninguna clase de interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.
- **Topología híbrida o mixta.** En esta topología las redes pueden utilizar diferentes tipologías para conectarse, como por ejemplo en estrella. La topología híbrida es una de las más comunes y se adquiere de la unión de varios tipos de topologías de red, de aquí el nombre de híbridas. Como, por ejemplo: en árbol, estrella-estrella, bus-estrella, etc.

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:

- **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.

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

N.º 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 TCP/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 "software" de aplicación, intercambien información.

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.

Los protocolos TCP/IP se puede dar en términos de capas, como se presenta a continuación:

- **Capa de aplicación**. La función la determina la aplicación que sea utilizada, es decir, proporcionar servicios de red que brindan la interfaz con el sistema operativo.
    - **FTP** ("File Transfer Protocol"): transferencia interactiva de archivos.
    - **TELNET**: inicio de la sesión de forma remota.
    - **HTTP** ("Hypertext Transfer Protocol"): transportar archivos que forman las páginas web de la "World Wide Web".
    - **SMTP** ("Simple Mail Transfer Protocol"): transmisión de mensajes de correo electrónico y archivos adjuntos.
    - **DNS** ("Domain Name System"): intrepidez del nombre de un host a la dirección IP.
- **Capa de transporte (TCP).** Garantiza que los paquetes lleguen sin errores y en secuencia.
    - **UDP** ("User Datagram Protocol"): crea una transmisión no fiable, o sea, que no está libre de errores.

- **TCP** (“Transmission Control Protocol”): forma una transmisión íntegra de datos. Es más complicado ya que contiene detección de errores y formas de recuperar los datos perdidos.

- **Capa de internet del modelo TCP/IP**. Suministra el paquete de datos (datagrama). Se relacionan algunos protocolos de la siguiente manera:
  - **IP** (“Internet Protocol”): factor principal de todo el modelo. Se establece para definir la dirección IP, comprobando así la ruta que tiene que seguir el paquete.
  - **ICMP** (“Internet Control Message Protocol”): proveer notificaciones y diagnóstico de errores cuando se malogran los datagramas IP.
  - **ARP** (“Address Resolution Protocol”): asiste al protocolo IP a guiar los datos solventando la dirección “hardware” o “MAC”.
  - **RARP** (“Reverse Address Resolution Protocol”): igual que el ARP pero al revés, o sea, dada la “MAC” te regresa la IP.
  - **NAT** (“Network Address Translation”): transforma la dirección IP privada a una pública.
  - **RIP** (“Routing Information Protocol”): es manejado por los “routers” para intercambiar información de las diferentes redes y ordenar con mayor eficacia los paquetes.
- **Capa física o de acceso a la red**. Está relacionada con componentes hardware que serán utilizados para la red y cómo enrutar los datos.
  - **CSMA/CD** (“Carrier sense multiple access / Collision detection”): Su función es gestionar la velocidad de transmisión de datos.

- **“Ethernet”:** Vincula el mensaje para conectarlo con la capa de red.
- **Protocolos de la capa física**: Establece la topografía de la web por medio de “routers”, “hubs” y “switches”.

1.6. Protocolos IPv4 e IPv6

El “Internet Protocol” versión 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 uno, por ejemplo 232.337.134.121. Luego, el DNS traduce esos datos en nombres de dominio como "ejemplo.es", ajustando todos los dígitos.

Por otra parte, está el “Internet Protocol” versión 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 es importante tenerlos presentes, al momento de adoptar el nuevo protocolo:

- **Más usuarios y mejores servicios.** Podrá tener un mayor número de equipos conectados a la red. Así mismo, tendrá un proceso técnicamente transparente para los usuarios de la red de comunicaciones y sus distintos servicios.

- **Mayor movilidad, mejor seguridad**. Tendrá la posibilidad de incrementar la movilidad de los usuarios al tener un número mayor de direcciones IP para la conectividad. En el mismo sentido, mejorará la seguridad a nivel de direccionamiento IP de la red, en virtud de la arquitectura del nuevo protocolo y sus servicios.
- **Reducción de costos y más aplicaciones y servicios**. Podrá reducir los costos al implementar la solución de IPv6; en este sentido, los costos podrían ser mayores de no implementarse el nuevo protocolo. Además, se facilitará la aparición de nuevas aplicaciones y servicios sobre una gran variedad de plataformas.
- **Nuevas tecnologías.** Gran número de direcciones IP para conexiones a internet con el mundo exterior, facilitando el crecimiento de nuevas tecnologías como el internet de las cosas, las ciudades inteligentes, redes de sensores, entre otras.
- **Amparo tecnológico de los PSI.** Los Proveedores de Servicio de internet, PSI, tendrán que preparar el proceso de transición de IPv6, mediante la creación de un "backbone" nativo de IPv6 que apoye a los clientes en el enrutamiento de las nuevas direcciones IPv6, a fin de garantizar la publicación de servicios y aplicaciones que se consideren pertinentes hacia internet.
- **Proveedores de servicio a cargo**. La implementación de IPv6 será un proceso gradual, cuya responsabilidad no será del gobierno, sino del proveedor del servicio de internet directamente y no deberá generar costos directos.

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.

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!

- **Estático.** Acceden a la configuración manual de las tablas de enrutamiento, las tablas no serán modificadas en forma dinámica, no tiene flexibilidad frente a fallas de los enlaces, no son fundamentales las cargas y procesos asociados a un protocolo de descubrimiento de rutas, se establecen fácilmente barreras de seguridad.

Ventajas	Desventajas
Suele ser muy segura debido a que es configurada manualmente. Es muy eficaz en redes pequeñas, en las que el administrador tiene total control de la red. Consume muy pocos recursos de sistema y la banda ancha.	Requiere mantenimiento constante por parte del administrador. Su manejo en redes grandes suele ser muy complejo y requiere mucho tiempo. No es escalable, por lo que no actualiza sus tablas de enrutamiento automáticamente.

- **Dinámico.** Se basa en la comunicación, por medio de "broadcasts", entre los "routers". Para hallar las mejores rutas, los "routers" utilizan el concepto de métrica y no se requiere mantener manualmente las tablas de rutas.

Ventajas	Desventajas
El tiempo de mantenimiento se reduce notablemente. Es eficaz tanto en redes grades como pequeñas. Es escalable, lo que reduce el trabajo del administrador de la red.	Su nivel de seguridad es mucho menor al de un enrutamiento estático. Se requiere, por parte del administrador, conocimientos complejos sobre enrutamiento dinámico. Consume muchos recursos del "router", así como banda ancha. Esto dependerá del tipo de protocolo que se suela usar.

2. Normatividad y estándares: ciberseguridad

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

La legislación define la norma:

> 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.
>
> Artículo 8 de la Ley 21/1992 de Industria

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.

Video 2. Prácticas e implementación de la ciberseguridad.

Enlace de reproducción del video

Síntesis del video: Prácticas e implementación de la ciberseguridad
Prácticas de implementación de la ciberseguridad. Las industrias involucradas en el ciberespacio se han preocupado por estudiar sobre la ciberseguridad. Como resultado de ello, diferentes entidades han abogado por el análisis desde un punto de vista metodológico para lograr el establecimiento de procesos y técnicas que garanticen la ciberseguridad en las empresas. Existen entidades encargadas de elaborar normatividad de nivel técnico, las cuales, apoyadas por equipos para la definición de estándares, permiten establecer un marco de trabajo para abordar problemas comunes en las organizaciones. La Organización Internacional de Normalización es la encargada de la creación de estándares internacionales. Está conformada por varias organizaciones internacionales de normalización para promover el uso de privativos industriales y comerciales a nivel mundial. La "Information Systems Audit and Control Association" es una asociación de orden internacional creada para apoyar y patrocinar el desarrollo de metodologías técnicas y certificaciones enfocadas en activos de auditoría y control en sistemas de información. El Comité Consultivo Internacional del Telegráfico y Telefónico promueve las recomendaciones técnicas sobre aspectos telefónicos, telegráficos e interfaces de comunicación de datos. El "National Institute of Standards and Technology" tiene como objetivo promover la innovación y la competencia industrial mediante avances en metrología, normas y tecnología para mejorar la estabilidad económica y la calidad de vida

Normatividad y estándares de la ciberseguridad. Complemente la información sobre la normatividad en la siguiente infografía.

https://ecored-sena.github.io/CF1_228138_Desarrollo_Implementacion_Soluciones_Transformacion_Digital/downloads/Infografia_Normatividad_y_estandares_de_la_ciberseguridad.pdf

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:

- **ISO 31000: Gestión del riesgo.** Directrices: esta normativa establece principios y guías para diseñar, implementar y mantener la gestión de los riesgos en forma sistemática y de transparencia de toda forma de riesgo, por ejemplo: financiera, operativa, de mercadeo, de imagen, y de seguridad de información.
- **ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información**. Esta norma se encuentra estructurada con 14 numerales de control de seguridad de la información que en su conjunto contiene más de 35 de categorías de seguridad principal y 114 controles.

Las actividades para la gestión del riesgo en la seguridad en la información son las siguientes:

- Establecimiento del contexto.
- Valoración del riesgo.
- Tratamiento del riesgo.
- Aceptación del riesgo.
- Comunicación del riesgo.
- Monitoreo y revisión del riesgo ((ICONTEC), 2009-08-19).

Los objetivos de la normatividad y estándares de la seguridad de la información son:

- **Identificar** los niveles de riesgo de ciberseguridad en la organización.
- **Hacer un plan de tratamiento** para la gestión de los riesgos que permita la disminución de los riesgos, facilitando lineamientos para gestionar los riesgos, apoyándose con las directrices de la ISO 27001 y 27002.

Alcance

La adopción de normatividad y estándares de gestión de riesgos de seguridad de la información tiene como alcance hacer el análisis de riesgos de los activos de información de las organizaciones determinando el impacto en los activos de información.

Características

La adopción de normatividad y estándares de gestión de riesgos de seguridad de la información, otorga una serie de características entre ellas:

- Identificar acontecimientos potenciales que afecte a la organización proporcionados por los niveles de riesgos.
- Proporcionar una seguridad razonable a la organización.
- Mejorar la agilidad de los sistemas de gestión de riesgos.
- Proporcionar una mayor confianza en la mitigación de riesgos.
- Mejora la comunicación y el flujo de información.

Aplicación

Se siguen la directrices y lineamientos dados por la norma:

- **ISO/IEC 27005:** seguridad de la información, ciberseguridad y protección de la privacidad.
- **ISO 31000:2018.** Gestión del riesgo. Directrices.

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.

A continuación, se presenta 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.

- **Proyectos.**
  - **Organizativo**: se refiere a la afección que se puede generar a la estructura de la organización, el método de trabajo que utilicemos o similares.
  - **Técnico**: se relaciona mucho con su nombre, ya que son proyectos con un contenido técnico significativo. Por ejemplo, securizar la página web corporativa.
  - **Regulatorio**: son proyectos enfocados a alinear algún aspecto concreto de la organización a alguna norma o regulación. Por ejemplo, los proyectos encaminados al cumplimiento de la LOPD y el RDLOPD.

- **Asesorías.** Se llevan a cabo después de un diagnóstico previo y su finalidad es brindar apoyo técnico en la toma de decisiones, relacionadas con las vulnerabilidades existentes, en materia de seguridad.
- **Servicios "outsourcing".** Para una organización es importante contar con un agente especializado en seguridad, que proteja y prevenga los ataques informáticos.
- **Contratación.** Regirse por la legislación favorece que en los contratos independientes, se asegure la información con cláusulas de confidencialidad y no divulgación.
- **"Freelance".** Es la persona que trabaja de forma independiente, ofreciendo sus servicios a empresas u otras personas, y quien maneja su tiempo y su forma de trabajar de manera autónoma. En ciberseguridad, un "Freelance". puede ayudar a complementar la seguridad digital teniendo en cuenta, entre otras, hacer copias de seguridad, trabajar con antivirus, usar escritorio virtual, proteger conexión a internet, reforzar seguridad de la web.
- **Acuerdos de confidencialidad.** Contrato de confidencialidad: cuando es necesario compartir la información de la organización, habrá que establecer las medidas de protección aplicables, por ejemplo: realizar una clasificación o utilizar técnicas de cifrado.

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.

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

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

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".

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 esta y que sea de valor para la organización.

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.

- **Baja.** Se considera baja cuando la clasificación de la información en todas sus propiedades es baja.
- **Media.** Se ubica en esta posición si la clasificación de la información de una de las propiedades es alta o nivel medio.
- **Alta.** Se determina cuando la clasificación es de dos, en todas las propiedades (confidencialidad, integridad, disponibilidad).

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.

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

- **Subestado de autentificación.** Presenta y conoce la autenticidad de los diferentes activos de información.
- **Subestado de confidencialidad.** Evitar que se divague, sin autorización, los activos de información.
- **Subestado integridad.** Muestra la protección sobre la modificación o destrucción, que no esté autorizada según los activos del dominio.
- **Subestado disponibilidad.** Protege contra el acceso no autorizado a 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.
- **El sistema mismo.** El propio sistema de información es considerado como uno de los tipos de activos.
- **Información generada.** Toda la información que se ha generado por la aplicación del Sistema de Gestión de Seguridad de la Información.
- **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.

- **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.

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.

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):

- **Sub-estado autentificación**
    - Baja
    - Normal
    - Alta
    - Crítica

- **Sub-estado confidencialidad**
    - Libre
    - Restringida
    - Protegida
    - Confidencial

- **Sub-estado integridad**
  - Baja
  - Normal
  - Alta
  - Crítica

- **Sub-estado 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.

A continuación, le presentamos algunas definiciones claves que favorecen la asimilación y conceptualización en lo referente a amenazas y vulnerabilidades informáticas.

- **Amenazas.** Cuando se habla de amenaza informática, se está haciendo referencia al aprovechamiento de la vulnerabilidad que se presenta para atacar o invadir un sistema informático.
- **Externas e internas.** Las amenazas informáticas para las organizaciones, generalmente, se adquieren mediante ataques; no obstante, hay otros tipos de amenazas como, por ejemplo, las amenazas internas (robos de información o uso inadecuado de los sistemas).
- **Vulnerabilidades.** Se relaciona con la debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder ingresar en los mismos y ejecutar actividades ilegales, robar información sensible o interrumpir su funcionamiento.
- **Actualización de sistemas de protección.** Hablar de vulnerabilidades es hablar de las principales causas por las cuales una empresa u organización puede llegar a ser víctima de ataques informáticos en contra de sus

sistemas. Por ello, se recomienda la actualización permanente a las últimas versiones disponibles de las aplicaciones informáticas; los sistemas de protección y operativos. Esto es fundamental, ya que contienen múltiples correcciones y ajustes sobre vulnerabilidades ya descubiertas.

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.

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 error en su diseño, o en su estructura; incluso es altamente frecuente que presenten fallas en su código, dando comienzo o cabida a cualquier vulnerabilidad.

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.

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.

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.

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

- **Del error a la amenaza.** El uso inadecuado de los sistemas y/o de sus funciones, posibilita cometer algunos errores que llegan a convertirse en amenazas para la empresa u organización.
- **Error del usuario, vulnerabilidad constante**. El error humano es otra causa de riesgos en ciberseguridad. La persona siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad, que genere una amenaza informática.
- **Necesidad de formación en ciberseguridad.** Se habla de la toma de control de los sistemas como el principal riesgo de este nivel. Otra razón por la cual se generan algunas vulnerabilidades es por la falta de formación en ciberseguridad, evidenciada en malas prácticas, caer en engaños publicitarios maliciosos, apertura de correos o información fraudulenta y eventos similares. Falsificación o venta de información sustraída, los ciberdelitos y la suplantación.
- **Phishing y otras amenazas.** Todas las gestiones o acciones equívocas llegan a ser una amenaza de potenciales ataques; entre los más comunes está el "phishing" (suplantación de identidad) u otros conexos o relacionados.

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.

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.

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 hacen 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.

Los niveles en los que se clasifican los riesgos:

- **Nivel bajo.** Tiene que ver con los ataques a la imagen, menosprecio, así como errores y fallos.
- **Nivel medio.** Se incrementan las capacidades ofensivas, siendo esta, la principal amenaza de este nivel. Además de la desfiguración de páginas web y la manipulación de información.
- **Nivel alto.** Se habla de la toma de control de los sistemas como el principal riesgo de este nivel, sin dejar a un lado el robo y publicación o venta de información sustraída, los ciberdelitos y la suplantación.
- **Nivel muy alto**. Puede generar la interrupción de los recursos IT y de otros servicios, con las graves consecuencias que puede tener para una organización, y la filtración de datos.
- **Nivel crítico**. Se habla del ciberespionaje como la gran amenaza de este nivel. El ataque proviene de APTs, campañas de "malware" interrupción

de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.

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.

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.

Características, impacto y análisis de riesgos. A continuación, se ha diseñado una guía sobre los riesgos, su impacto y probabilidad, su análisis y tratamiento. Descarga la siguiente infografía. https://ecored-sena.github.io/CF1_228138_Desarrollo_Implementacion_Soluciones_Transformacion_Digital/downloads/infografia_ciberseguridad_Caracteristicas.pdf

Para estudiar a profundidad las técnicas de tratamiento de riesgos y afianzarse en la adopción de controles de seguridad, se recomienda 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

9.3. Técnicas del tratamiento de riesgos

La etapa de tratamiento de los riesgos consiste en comparar los niveles del riesgo encontrados durante los procesos de identificación y análisis, con los criterios previamente establecidos. En esta etapa se realiza la priorización de los riesgos para futuras acciones, igualmente se contemplan las decisiones a tomar, conforme a las consideraciones de apetito o tolerancia al riesgo desde la alta dirección.

Si el riesgo resultante es considerado bajo o aceptable, debe ser controlado con un mínimo tratamiento, sin dejar de ser monitoreado periódicamente, para asegurar que se mantengan en niveles aceptables.

Una vez se obtiene el mapa de riesgos, se sigue con el paso de tratamiento, donde se derivan planes de mejora a desarrollar, reconociendo cuáles serán las acciones para el tratamiento del riesgo, valorando estas opciones y preparando los planes de tratamiento del riesgo e implantarlos.

Los siguientes son los mecanismos para el tratamiento de los riesgos:

- **Evitar.** Es la decisión de no proceder con la actividad que probablemente genere el riesgo.
- **Transferir.** Es buscar un respaldo y compartir con un tercero alguna proporción del riesgo a través de contratos, pólizas, etc.
- **Reducir y controlar.** Es establecer mecanismos de control que reduzcan el riesgo, puede ser mediante controles preventivos, correctivos, disuasivos, etc.
- **Asumir o retener.** Luego de que el riesgo ha sido reducido o transferido, puede quedar un riesgo residual el cual se debe retener.

Una vez identificadas las acciones a realizar, es necesario llevar a cabo la implementación de los planes de tratamiento; lo ideal es que la responsabilidad por el tratamiento del riesgo recaiga en aquellos más capaces de controlar el riesgo o que puedan tomar decisiones sobre estos.

Llevar a feliz término la implementación de un plan de tratamiento del riesgo requiere un mecanismo gerencial muy efectivo con la suficiente jerarquía en la organización, de modo que puedan asignarse las responsabilidades individuales de las acciones y monitorearlas de acuerdo con el criterio especificado.

En las técnicas del sistema de tratamientos de riesgos se debe garantizar lo siguiente:

- Un funcionamiento correcto de la organización.
- Revisiones internas efectivas.
- Controles legales actualizados con las leyes y reglamentos vigentes.

Además, se pueden establecer estrategias para evitar los riesgos y minimizar el impacto o la frecuencia de ocurrencia del riesgo; así, al analizar el nivel del riego se podrá tomar la decisión para el mecanismo de tratamiento y la implementación del control para mitigarlo, articulando todo esto, mediante la política de control y con el plan de mejora de la organización.

Es importante destacar que el paso final de la gestión de riesgos está asociado al monitoreo y revisión, donde es necesario monitorear los riesgos, la efectividad del plan de tratamiento del riesgo, las estrategias y el sistema gerencial establecido para controlar la implementación.

Las revisiones continuas son esenciales para asegurar que el plan de tratamiento permanezca consistente con la realidad, por lo que es necesario implementar mecanismos periódicos de monitoreo, tanto para las implementaciones de tratamiento, controles y riesgos de niveles altos, como para la definición y el seguimiento a todo en un mapa de riesgos.

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.

Las pruebas de penetración de un “hacker” ético, permiten evaluar vulnerabilidades, analizar y categorizar las debilidades explotadas y proveer recomendaciones, con 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.

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.

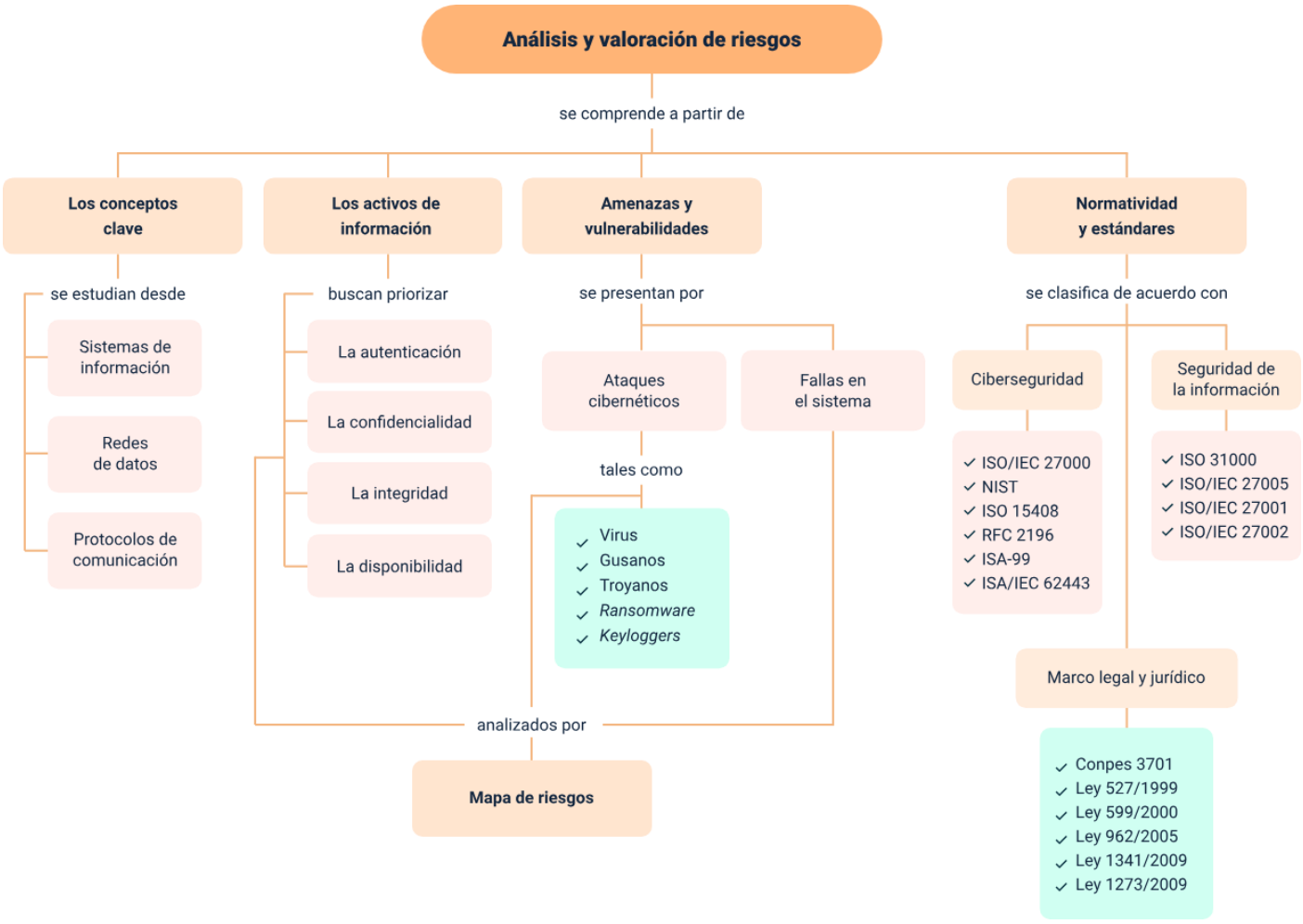
10.2. Tipos de pruebas de penetración

Dentro del ejercicio del “ethical hacking”, existen tres tipos de pruebas de penetración: caja negra, caja blanca y caja gris. Descubra las particularidades de cada uno 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 datos privilegiados tendría de manera realista.

Síntesis

A continuación, se presenta el diagrama que representa el resumen de las temáticas que están desarrolladas en el componente formativo:



El mapa conceptual representa el análisis y valoración de riesgos, que se comprende a partir de conceptos clave como sistema de información, red de datos y protocolos de comunicación. Asimismo, se trabajan los activos de información, buscando priorizar la autentificación, la confidencialidad, la integridad y la disponibilidad. Posteriormente, se abordan las amenazas y vulnerabilidades a través de

ataques cibernéticos, como los virus, gusanos, troyanos, “ransomware” y “keyloggers”, que son analizados mediante un mapa de riesgos.

Desde la perspectiva de la normatividad y estándares, la ciberseguridad se clasifica de acuerdo con diferentes normas, tales como la norma ISO 27000, la ISO 15408, la ISO 31000 y algunas otras como la Compres 3701 y la Ley 1273 de 2009.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Normatividad y estándares: ciberseguridad 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
Normatividad y estándares: ciberseguridad 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
Amenazas y vulnerabilidades	Gómez, V., Á. (2015). Auditoría de seguridad informática. RA-MA Editorial.	Libro	https://www-ebooks7-24-com.bdigital.sena.edu.co/?il=6422&pg=1
Riesgos	Gómez V., Á. (2015). Seguridad en equipos informáticos. RA-MA Editorial.	Libro	https://www-ebooks7-24-com.bdigital.sena.edu.co/?il=8105&pg=1
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
“Ethical Hacking”	Astudillo, B. K. (2019). Hacking ético: ¡Cómo convertirse en hacker ético en 21 días o menos! Ediciones de la U.	Libro	https://www-ebooks7-24-com.bdigital.sena.edu.co/?il=10047&pg=1

Glosario

Activos de información: están relacionados con la seguridad de la información, hacen referencia a cualquier información o dispositivo que tenga que ver con el tratamiento de esta y que sea de valor para la organización.

Auditoría: 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 la auditoría de SGSI es investigar, de manera objetiva, si existe algo que esté mal realizado. 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": 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”: “software” diseñado para comprometer la seguridad de la información, como la utilidad y preservación del equipo.

Riesgo: 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: 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.

Tratamiento de riesgos: medidas y controles que se implementan para mitigar el impacto o la frecuencia de ocurrencia de un riego.

Virus informático: “software” que se instala en un dispositivo sin el consentimiento del usuario, con el fin de alterar el funcionamiento.

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 de España. (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 de Colombia. (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

Projete. (s.f.). Amenazas y vulnerabilidades. https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Diana Carolina Triana Guarnizo	Instructor	Centro de Gestión Industrial - Regional Distrito Capital
Juan Carlos Cárdenas Sánchez	Instructor	Centro de Gestión Industrial - Regional Distrito Capital
Gloria Esperanza Ortiz Russi	Diseñador Instruccional	Centro de Diseño y Metrología - Regional Distrito Capital
Fabián Leonardo Correa Díaz	Diseñador Instruccional	Centro Industrial del Diseño y la Manufactura - Regional Santander
Ana Catalina Córdoba Sus	Asesor Metodológico	Centro Industrial del Diseño y la Manufactura - Regional Distrito Capital
Yerson Fabian Zarate Saavedra	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Francisco José Lizcano Reyes	Desarrollador Fullstack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Storyboard e Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Mary Jeans Palacio Camacho	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carlos Eduardo Garavito Parada	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Camilo Andrés Bolaño Rey	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruíz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander