**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| **PROGRAMA DE FORMACIÓN** | **Tecnología en Desarrollo e Implementación de Soluciones para la Transformación Digital** |

|  |  |
| --- | --- |
| **NÚMERO DEL COMPONENTE FORMATIVO** | 1 |
| **NOMBRE DEL COMPONENTE FORMATIVO** | CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN |
| **BREVE DESCRIPCIÓN** | |  | | --- | | El manejo de los datos en el entorno mundial juega un papel fundamental en el desarrollo de las actividades cotidianas de empresas y en general del ámbito productivo; esto ha generado grandes ventajas en dado que la tecnología es la herramienta que soporta la gestión de datos, sin embargo, en la actualidad se ha notado que en las redes de datos e infraestructura tecnológica, aplicaciones informáticas y digitales ha ido aumentando la inseguridad, convirtiéndose en un problema crítico, por tanto la anticipación a este fenómeno es esencial y debe ser comprendido para poder administrar y gestionar los activos de información e infraestructura. | |
| **PALABRAS CLAVE** | Ciberseguridad, información, políticas, riesgo |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPETENCIA** | **220501108 - Diagnóstico del estado actual de la ciberseguridad de la organización** | **RESULTADOS DE APRENDIZAJE** | 220501108 -01 Determinar métodos de análisis y valoración de riesgos de ciberseguridad, de acuerdo con estándares internacionales y normatividad nacional. |

|  |  |
| --- | --- |
| **AREA OCUPACIONAL** | No Aplica |
| **IDIOMA** | Español |

1. **TABLA DE CONTENIDOS:**

Introducción

* 1. **Fundamentos de redes y networking**
  2. Las redes de datos
  3. Elementos que componen una red
  4. Tipos de Redes de Datos
  5. Topologías de red
  6. Modelos de referencia
  7. Direccionamiento IP
  8. **Seguridad de la información**

2.1 Generalidades

2.2 Principios

2.2.1 Confidencialidad

2.2.2 Integralidad

2.2.3 Disponibilidad

2.3 Vulnerabilidades

2.3.1 Tipos de vulnerabilidades

2.3.2 Humanas

2.3.3 Naturales

2.3.4 Físicas

2.3.5 de comunicación

2.3.6 De hardware

2.3.7 De software

2.3.8 De almacenamiento

2.4 Amenazas Informáticas

2.4.1 Inyección SQL

2.4.2 DDoS – Denegación de servicio

2.4.3 Cross-site scripting (XSS)

2.4.4 Interceptación

2.4.5 taques de Fuerza Bruta

2.4.6 Inadecuada seguridad

2.4.7 Ingeniería social

* 1. **Hacking ético**

3.1 Propósito del Hacking ético

3.2 Tipos de Hacking

3.2.1 Hackers Black Hat

3.2.2 Hackers White Hat

3.2.3 Hackers Grey Hat

3.2.4 Hackers Newbies

3.2.5 Hacktivista

* 1. **Daño Informático**

4.1 Delito Informático

4.2 Tipificación de los delitos informáticos

* 1. **Ciberseguridad**

5.1 Definición

5.2 Generalidades

5.2.1 Prevención

5.2.2 Localización

5.2.3 Reacción

5.3 Fases de implementación de ciberseguridad

5.3.1 Entendimiento de la organización.

5.3.2 Análisis de Riesgos.

5.3.3 Plan de acción

5.3.4 Implementación

1. **DESARROLLO DE CONTENIDOS:**

Introducción

En este módulo se estudiarán los principios básicos de la seguridad de la información y su evolución a la ciberseguridad, de igual manera se conocerán y apropiarán las normas y estándares internacionales utilizados y recomendados.

1. **Fundamentos de redes y neworking**
   1. **Las redes de datos**

Podemos definir las redes de computadoras como dos o más dispositivos (computadoras, tablets, celulares, es decir cualquier dispositivo que pueda ser conectado, ya sea por cables (alámbricas) o por wifi (inalámbricas), con el propósito de transmitir, intercambiar o compartir datos, recursos e información.

Las redes informáticas tienen la capacidad de dar información para cada propósito de negocios, entretenimiento e investigación también da la posibilidad de utilizar una única conexión a internet en varios ordenadores, compartir impresora y otros periféricos, enviar y recibir mensajes y pasar archivos a otros ordenadores sin requerir de una memoria usb, cd u otro elemento.

* 1. **Elementos que componen una Red**

Es importante conocer de manera general cuales son los componentes que hacen parte de las redes de datos, esto nos será de gran utilidad y ayuda para identificar posibles fallas y sus respectivas soluciones.

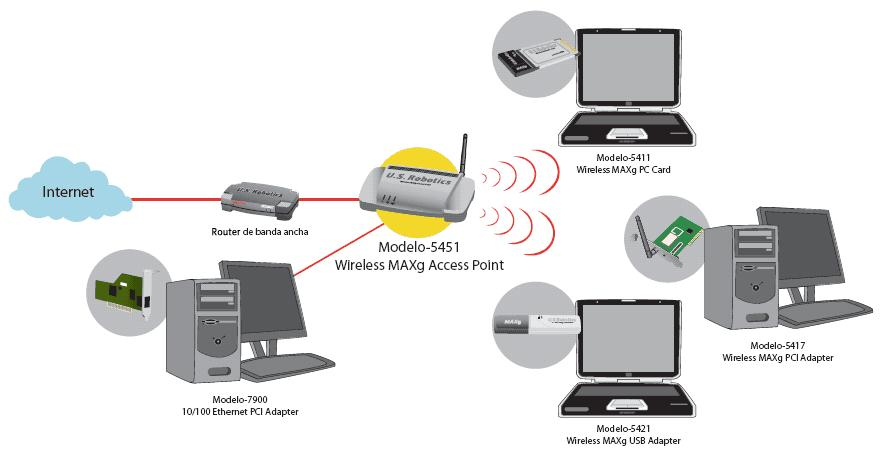


Imagen 1: Coponentes de una red, tomado de <https://estecnoinformatic.com/c-informatica->basica/elementos-de-una-red-funcion-principal-grafica-y-mas/

* + 1. El servidor

Es quizá de los más importantes en las redes de datos, es generalmente una computadora con buenas características de hardware y software que se encarga de proveer recursos o servicios a las otras computadoras recibiendo y procesando las peticiones o solicitudes hechas por los equipos denominados clientes a quienes da respuesta a través el uso de las redes ya sean locales o por internet. Podemos encontrar diferentes tipos de servidores como correo electrónico, servicios de almacenamiento, servidores web de bases de datos, entre otros.

Este tipo de elemento trabaja en una arquitectura que denominamos **CLIENTE – SERVIDOR,** donde el cliente es quien demanda algún recurso servicio y el servidor es el encargado de proporcionárselo.

* + 1. Estación de Trabajo o Cliente

Las estaciones de trabajo o clientes en una red son aquellos dispositivos informáticos utilizados para realizar una labor especifica, son los elementos con los generalmente se realizan los trabajos de tipo, empresarial, científico, entretenimiento, entre otros. Estos están conectados entre sí a través de servidores para facilitar el intercambio de recursos y servicios.

Generalmente cuando hablamos de estaciones de trabajo o clientes nos imaginamos únicamente computadoras, sin embargo, dado el avance y desarrollo tecnológico hoy es cualquier dispositivo que pueda conectarse a una red y pueda acceder a los servicios estos pueden ser: Tablet, Celulares, televisores y cualquier otro electrodoméstico que hoy en día viene dotado de una tarjeta de red.

* + 1. Tarjetas de Red

Este dispositivo generalmente viene incluido en la estación de trabajo o cliente, es el elemento de red que permite que el dispositivo pueda conectarse a la red ya sea de manera cableada o inalámbrica en el caso del wifi.

Imagen que contiene electrónica, computadora

Descripción generada automáticamente  

* + 1. Dispositivos Intermedios

Estos son elementos que permiten hacer la interconexión entre los diferentes dispositivos de la red facilitando su comunicación son algunos de los dispositivos intermediarios los siguientes:

**Router**(Enrutador): es el elemento encargado de buscar el mejor y mas optimo camino para transmitir o levar una señal desde un dispositivo hacia otro o desde un dispositivo hacia otra red, otra de sus funciones es permitir que varios equipos ya sea en el hogar o en la oficina compartan una misma salida hacia internet.

**Switch:** son elementos de red de tipo digital que permiten la interconexión de varios dispositivos en una misma red, regularmente facilitan formar lo que conocemos como una Red de Área Local (LAN) y obedecen a un estándar de red denominado Ethernet.

**Access Point (Punto de Acceso):** Son dispositivos que cumplen la misma función del switch pero para conexiones inalámbricas entre equipos o dispositivos, regularmente interconectan dispositivos móviles o tarjetas de red inalámbricas.

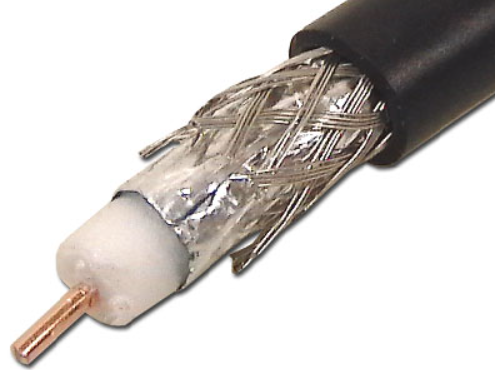
* + 1. Medios de Transmisión

Los medios de trasmisión son aquellos elementos que facilitan la conexión físicamente entre los diferentes elementos que conforman una red, podemos clasificarlos en dos grandes familias los guiados y los no guiados.

Los medios de transmisión guiados son todos aquellos que utilizan un medio físico para la recepción y envío de las señales entre los diferentes dispositivos y estos a su vez se clasifican en dos tipos los que son de cobre que pueden ser par trenzado o coaxial y las fibras ópticas.

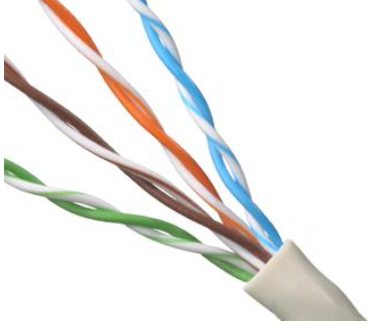
En el caso de los medios de transmisión no guiados encontramos todos aquellos que utilizan como medio para enviar y recibir la señal el aire o un medio inalámbrico, de manera muy general se explican a continuación los diferentes medios de transmisión mencionados.

**Cable coaxial**: este medio es muy similar al cable utilizado en las antenas de televisión, contiene un hilo de cobre en la parte central y es protegido con una malla metálica que hace la función de puesta a tierra y ambos elementos están separados por una chaqueta de plástico, protegido finalmente por una cubierta exterior.



Imágen 2: Cable Coaxial

**Cable Par trenzado:** es un medio que contiene hilos de cobre (pares) aislados por una cubierta plástica y trenzados entre sí, regularmente son muy utilizados a nivel empresarial ya que por sus cualidades permite reducir o disminuir la interferencia, factor que afecta de manera considerable el correcto funcionamiento de las redes de datos.



Imágen 3: Cable par trenzado

Fibra óptica: Es un medio de comunicación que usa la luz confinada en una fibra de vidrio, para así transmitir cantidades grandes de información que van por el orden de Gigabits (1 x 109 bits) por segundo. Para la transmisión de los haces de luz se usa una fuente de luz como un LED o un diodo láser.



Imágen 4: Fibra Optica

* 1. Tipos de Redes de Datos

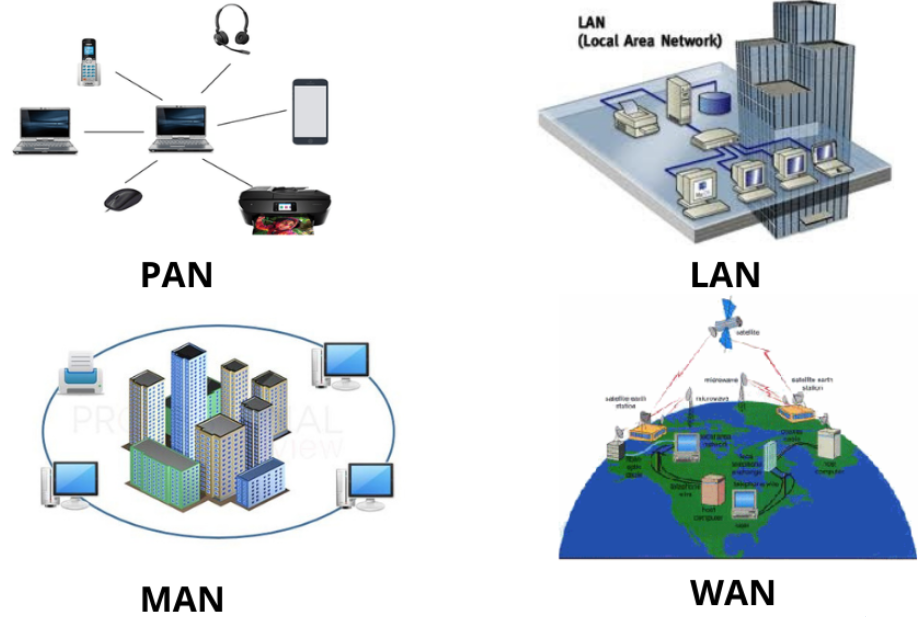


Imagen 5: Tipos de redes de datos, tomado de https://grupodct.mx/?fbclid=IwAR2reKzVS-9yqLCL4zQMvPig9bcxVrJQI3EaoSxZAZPv6P73MFp\_cgUgUwo

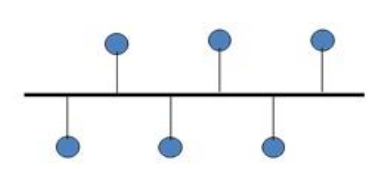
En la medida que evolucionaron las redes de datos ya fuera por las necesidades y avances tecnológicos fue necesario desarrollar diferentes tipos de redes que satisficieran las nuevas y cada vez mayores necesidades, a continuación, se describen las redes más comúnmente utilizadas:

* + - LAN (red de área local): tiene la función de unir varios ordenadores y dispositivos conectados a un servidor en una área o espacio geográficamente limitado a un campus, edificio u hogar.
    - 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 por ejemplo en una oficina o vivienda normalmente están asociadas al uso de dispositivos como celulares o medios de alcance corto como infrarrojos o bluetooth.
  1. Topologías de red

La topología de define como se conectan y comunican los diferentes dispositivos en una red. La topología puede ser física o lógica. La topología física se refiere a la disposición física de los dispositivos y medios de red que los interconectan. Las topologías físicas más comunes son las siguientes:

Topología de Bus

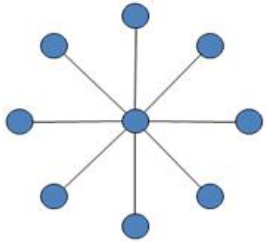
En este tipo de topología todos los dispositivos de la red se interconectan usando el mismo medio de transmisión que en este caso es un cable llamado de conexión central. Como es un solo cable al final de este se debe de poner un terminador para evitar que la señal se reflexione.



Imágen 6: Topología física de Bus

Topología de estrella

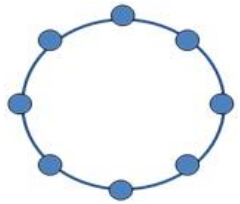
Es quizá la topología más común al momento de implementar redes LAN. En esta topología todos los dispositivos se conectan a través de un cable por dispositivo o una señal inalámbrica con un dispositivo central (Hub, Switch, Access point).



Imágen 7: Topología física de Estrella

Topología en anillo

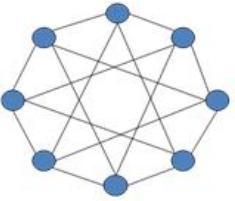
En esta topología cada dispositivo se interconecta con dos vecinos y así sucesivamente hasta formar un anillo, para la transmisión de los datos cada dispositivo requiere tener un permiso para poder transmitir denominado token. Los datos viajan de dispositivo en dispositivo hasta encontrar el destinatario.



Imágen 8: Topología Física de anillo

Topología de Malla

En esta topología cada dispositivo de red se interconecta con todos los demás a partir de un cable independiente para buscar tolerancia a fallas. En la práctica cuando se requieren un diseño de red redundante se implementa una topología en malla parcial, por los costos en los que se incurre al implementar una en malla completa.



Imágen 9: Topología Física de Malla

* 1. Modelos de Referencia

Un modelo de referencia proporciona una referencia común para mantener consistencia en todos los tipos de protocolos y servicios de red. El propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados más que entrar en los detalles de las especificaciones técnicas requeridas por cada capa. El modelo de referencia para las redes de comunicaciones es el modelo OSI (Interconexión de Sistemas Abiertos.

Modelo OSI

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

Tabla 1: Modelo de Referencia OSI, tomado de Guía de administración del sistema: servicios IP (2010).

|  |  |  |
| --- | --- | --- |
| **Capa** | **Nombre de capa** | **Descripción** |
| 7 | Aplicación | Se compone de los servicios y aplicaciones de comunicación estándar que puede utilizar todo el mundo. |
| 6 | Presentación | Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el sistema. |
| 5 | Sesión | Administra las conexiones y terminaciones entre los sistemas que cooperan. |
| 4 | Transporte | Administra la transferencia de datos. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos. |
| 3 | Red | Administra las direcciones de datos y la transferencia entre redes. |
| 2 | Vínculo de datos | Administra la transferencia de datos en el medio de red. |
| 1 | Física | Define las características del hardware de red. |

Modelo TCP/IP

Fue el primer modelo de protocolo en capas para comunicaciones de red. Fue desarrollado en la década de los 60 por el departamento de defensa de los EE. UU (DoD), con el objetivo de crear una red de comunicaciones que funcionara incluso en condiciones de guerra.

Aunque el modelo OSI es universalmente reconocido, el estándar histórica y técnicamente reconocido para Internet es el modelo TCP/IP (Protocolo de Control de Transferencia / Protocolo de Internet).

El modelo TCP/IP consiste en cuatro capas como se muestra a continuación.

Tabla 2: Modelo TCP/IP

|  |  |  |
| --- | --- | --- |
| **Capa** | **Nombre de capa** | **Descripción** |
| 4 | Aplicación | Representa los datos para el usuario y el control y codificación |
| 3 | Transporte | Admite la interconexión de diferentes dispositivos entre las distintas redes |
| 2 | Internet | Determina la mejor ruta a través de la red |
| 1 | Acceso a la Red | Controla los dispositivos de hardware y los medios de transmisión utilizados en la red. |

Al ser Los protocolos TCP/IP son un conjunto de reglas para formatos de mensajes y procedimientos que permiten que el hardware y el software de aplicación intercambien información. El conjunto de protocolos TCP / IP se puede entender en términos de capas (o niveles). A continuación, se presentan los protocolos de acuerdo a cada capa del modelo TCP/IP

Imagen de la pantalla de un celular con letras

Descripción generada automáticamente con confianza media

Imagen 10: protocolos TCP/IP

* 1. Direccionamiento IP

Para hablar de direccionamiento IP debemos entender que es una dirección IP, esta es un identificador único que corresponde a cada dispositivo conectado o perteneciente a una red de datos de tipo local o externa, IP significa “protocolo de Internet” que es el conjunto de reglas y estándar que rigen las comunicaciones y la forma en que se envían y reciben datos a través de una red local o internet.

Las direcciones IP son la forma de identificar un dispositivo y permitir el envío de información entre dispositivos en la red. Estas direcciones contienen información de la ubicación tanto en el origen como el destino al momento de establecer una comunicación. El Internet requiere poder diferenciar entre distintas computadoras, enrutadores, dispositivos y sitios web. Las direcciones IP proporcionan una forma de hacerlo y forman una parte esencial de cómo funciona Internet.

Las direcciones IP son un conjunto de números separados por un punto, en total las direcciones IP tienen cuatro conjuntos de números que van desde el valor 0 hasta el valor 255 siendo este el máximo valor que puede tener un conjunto. Por lo tanto, los rangos s de direcciones IP van desde el valor mínimo que obedece a 0.0.0.0 hasta 255.255.255.255.

Por su tamaño o capacidad total máxima de direcciones IP estas se pueden clasificar en Direcciones IP v4 y direcciones IP V6, debido a la permanente y exponencial demanda de solicitudes de acceso a internet fue necesario pasar del modelo de direccionamiento IPv4 al IPv6 a continuación se mostrarán las principales diferencias entre las dos.

* Tamaño: mientras que las direcciones IPv4 utiliza un tamaño de 32 bits, IPv6 utiliza un formato de 128 bits
* Notación: para IPv4 su notación es decimal, mientras que para IPv6 es hexadecimal, es decir pasamos de un formato por bloque de 8 posibles valores a bloques de 16 bits.
* IPv6 Integra Ipsec como un elemento de seguridad que funciona en la capa de red lo que garantiza la protección de las comunicaciones enviadas y recibidas por su cifrado.
* IPV6 integra un elemento llamado QoS (Calidad del servicio), esta característica permite diferenciar o distinguir paquetes por tipos de protocolos y servicios lo que facilita dar cierta prioridad al tráfico.
* El IPv6 permite una administración de red mas sencilla ya que integra una configuración automática de direcciones, por defecto toda tarjeta de red ya tiene su dirección IPv6 integrada.
* Las direcciones IPv4 se dividen en “clases” con redes de Clase A para algunas redes enormes, redes de Clase C para miles de redes pequeñas y redes de Clase B que están entre las dos primeras. IPv6 utiliza la subcompensación para ajustar los tamaños de la red con una asignación determinada de espacio de dirección.

Las direcciones IP pueden ser considerada de dos tipos las privadas y las públicas, las primeras son las utilizadas a nivel local ya sea en la empresa o el hogar, son direcciones controladas y administradas por el usuario o administrador de la red y son visibles únicamente de manera local, las segundas son las direcciones que son asignadas por los ISP (Internet Service Provider) cuando adquirimos una conexión a internet estas son visibles por cualquier internauta y usualmente están configuradas en los dispositivos de interconexión como routers, firewall o servidores.

En cuanto a su configuración las direcciones IP pueden ser dinámicas o fijas, las primeras son direcciones que van cambiando cada vez que el dispositivo establece una conexión a la red local o internet, y se utiliza cuando en la red hay muchos clientes o el numero de clientes es mayor al número de direcciones IP ya que es poco probable que todos se conecten al mismo tiempo. Entre sus ventajas se encuentra un mayor nivel de seguridad y privacidad en la red, además de que su configuración es automática, sin embargo, la probabilidad de que la conexión se interrumpa es más elevada que en una IP fija.

Por otra parte, las direcciones IP fijas son asignadas a un dispositivo de por vida, es decir, jamás cambiará, y esto aplica tanto para direcciones IP públicas como privadas, A pesar de que son de mayor confianza y estabilidad, y te permiten una mayor velocidad de descarga, llegan a presentar ciertos inconvenientes, empezando por la vulnerabilidad. Al ser estáticas, los hackers tienen más tiempo para atacar equipos con este tipo de IP.

1. **Seguridad de la información**
   1. Generalidades

El concepto de seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados. Soriano, M. (2014).

Si bien son complementarias se debe diferenciar los conceptos de seguridad de la información, seguridad informática y seguridad en la red, La seguridad informática es el nombre genérico para el conjunto de herramientas diseñadas con el fin de proteger los datos almacenados en un equipo y evitar ataques de piratas informáticos.

Seguridad en la red es el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicaciones.

Las diferencias entre seguridad de la información, seguridad informática y seguridad en la red radican principalmente en la aproximación al tema, metodologías utilizadas y el ámbito en que se centra. La seguridad de la información tiene que ver con la confidencialidad, integridad y disponibilidad de los datos, independientemente de su formato. La seguridad informática se orienta a garantizar la disponibilidad y el correcto funcionamiento de un sistema informático. La seguridad en la red se centra en la protección de los datos durante su transmisión.

* 1. Principios

Como se mencionó anteriormente la seguridad de la información se centra en garantizar lo que en el mundo de seguridad se conoce como la triada conocida por sus siglas CIA, que nada tienen que ver con una famosa agencia de estados unidos, se le da este nombre ya que corresponde a las iniciales de los principios que sustentan la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

* + 1. Confidencialidad

La confidencialidad se refiere a los esfuerzos de una organización para mantener sus datos privados o secretos. En la práctica, se trata de controlar el acceso a los datos para evitar su divulgación no autorizada.

Esto implica asegurarse que sólo aquellos autorizados tengan acceso a activos específicos y, que quienes no están autorizados, sean impedidos activamente de obtener acceso.

* + 1. Integralidad

En seguridad informática, la integridad consiste en garantizar que los datos no hayan sido manipulados y, por lo tanto, sean confiables.

Garantizar la integridad implica proteger los datos en uso, en tránsito (por ejemplo, al enviar un correo electrónico o al cargar o descargar un archivo) y al almacenarlos, ya sea en aparatos físicos o en la nube.

* + 1. Disponibilidad

Los sistemas, aplicaciones y datos son de poco valor para una organización y sus clientes si no son accesibles cuando los usuarios autorizados los necesitan.

En pocas palabras, la accesibilidad significa que las redes, los sistemas y las aplicaciones están en su pleno funcionamiento. Ello garantiza que los usuarios autorizados tengan acceso oportuno y fiable a los recursos cuando los necesiten.

* 1. Vulnerabilidades

Es una debilidad o fallo en un sistema de información que puede ser ocasionado por un error de diseño, programación, configuración o humano que puede ser utilizado por una persona mal intencionada poniendo en riesgo la seguridad de la información permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta.

Los siguientes son algunos ejemplos:

* Un servicio de un sistema de computación corriendo en un determinado puerto lógico.
* Sistemas operativos y aplicaciones sin actualizaciones lo que generan múltiples vulnerabilidades.
* Una red Wifi abierta o con sistemas de autenticación muy débiles.
* Un puerto de comunicaciones abierto de manera innecesaria en un firewall.
* Controles de acceso físico y lógico insuficiente o inexistentes.
* Uso de contraseñas débiles sin la aplicación de una política de gestión de contraseñas.
  + 1. Tipos de vulnerabilidades

De manera general podemos clasificar las vulnerabilidades de la siguiente manera:

* + 1. Humanas

Como lo indica su nombre son fallas humanas ocasionadas de manera intencional o por desconocimiento como ejemplo podemos mencionar: fallos en la gestión d configuraciones, sistemas o métodos de validación y autenticación, asignación de permisos.

* + 1. Naturales

Hace referencia a cualquier tipo de condición Natural que afecte los equipos y/o servicios pueden ser, por ejemplo: terremotos, inundaciones, incendios, entre otros.

* + 1. Físicas

Son aquellas que se presentan en el mismo lugar donde se encuentran alojados y se almacenan los datos, los servicios o sistemas un ejemplo de esta vulnerabilidad puede ser: desconectar el suministro eléctrico, desconexión de un cable o medio de transmisión, conexión de pen drives con software malicioso o mal intencionado, entre otros.

* + 1. de comunicación

Están relacionados a fallos presentados en los medios de transmisión utilizados transmitir y recibir las conexiones en cuanto a transmisión y recepción de datos, por ejemplo: falla en la fibra, cobre o medios inalámbricos utilizados para las conexiones.

* + 1. De hardware

Pueden ocasionarse por fallas en la fabricación y configuración que puede comprometer los datos.

* + 1. De software

Se pueden generar por una mala configuración o poca calidad en el código al momento de programar las aplicaciones.

* + 1. De almacenamiento

Ocasionados por fallas en construcción, configuración o disposición de los medios como discos duros, memorias USB o cualquier otro medio de almacenamiento utilizado.

En términos generales las vulnerabilidades del software y las comunicaciones en cualquiera de los ámbitos antes descritos están directamente relacionadas con el concepto de “MALWARE”, o software malicioso el cual es diseñado con fines específicos de intentar explotar o dañar cualquier dispositivo, software, servicio o red.

Algunos ejemplos comunes de este tipo de software son:

* Virus informáticos: es un tipo de software malicioso diseñado y construido para modificar el comportamiento o desempeño de un recurso tecnológico.
* Gusanos: son códigos maliciosos diseñados para reproducirse y ubicarse en varias ubicaciones del recurso tecnológico con el fin de hacer colapsar los dispositivos y redes informáticas.
* Troyanos: son códigos maliciosos diseñados para engañar al usuario haciéndose pasar por software validos para que al hacer clic o cualquier otra acción se instalen y puedan desarrollar la actividad para que fueran programados.
* Rasonware: es un tipo de malware o código malicioso diseñado para hacer un secuestro de los datos del usuario lo que le impide el acceder a ellos y regularmente exigen un pago para liberarles y permitirles de nuevo el acceso a dichos recursos.
* Keyloggers: es un tipo de software malicioso hecho para capturar las pulsaciones de las techas por parte del equipo infectado, de esta manera buscan robar cuentas de usuario y contraseñas de acceso a los sistemas informáticos.

* 1. **Amenazas Informáticas**

Definimos la amenaza como todo elemento o acción capaz o que puede atentar contra la seguridad de la información afectando cualquiera de los pilares como lo son la Integridad, la disponibilidad y confidencialidad.

Para que una amenaza se pueda desarrollar requiere de la existencia de vulnerabilidades que puedan ser aprovechadas independientemente de si se compromete o no la seguridad.

Son causales del aumento de amenazas de tipo intencionales la falta de entrenamiento y capacitación a los usuarios, la falta de concienciación, la ingeniería social y sobre manera la rentabilidad de producir amenazas intencionadas.

Las amenazas pueden categorizarse en dos tipos:

* Amenazas Intencionadas: son aquellas que son producidas de intencionalmente por un atacante en búsqueda de apoderarse de datos e información o de producir algún tipo de cambio en la operación normal de un servicio. Por ejemplo, la aplicación o uso de códigos maliciosos, aplicación de técnicas de ingeniería social para buscar la suplantación de identidad.
* Amenazas no Intencionadas: Es cuando se producen acciones u omisiones de acciones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales).

De acuerdo con el origen de la amenaza estas se pueden clasificar en:

* Amenazas externas: son aquellas que provienen de afuera de la organización y en muchos de esos casos escapan de la gestión y control por parte de las áreas de tecnología, podemos mencionar como ejemplo los virus, los gusanos, los troyanos.
* Amenazas Internas: son aquellas que se ejecutan desde el interior de las organizaciones, permiten ser controladas hasta cierto grado por las áreas de tecnología algunos ejemplos son: la suplantación de identidad, el acceso abusivo o no autorizado a los datos, el robo de datos entre otras.

A continuación, se describen de manera muy general algunas de las amenazas mas comunes a las cuales nos enfrentaremos en la seguridad de la información.

* + 1. Inyección SQL

Es una amenaza muy común que utiliza vulnerabilidades presentes en los formularios de acceso a datos para inyectar instrucciones que permitan conectarse y tener acceso a las bases de datos de las diferentes aplicaciones en búsqueda de poder robar datos e información.

* + 1. DDoS – Denegación de servicio

Este tipo de amenaza lo que busca es enviar un numero alto de peticiones al servidor o servicio en búsqueda de que este no pueda dar respuesta oportuna a tantas peticiones concurrentes lo que le impedirá a un usuario real acceder o recibir respuesta del servicio.

* + 1. Cross-site scripting (XSS)

Se presenta cuando se hace un tipo de inyección de programa maligno o malware que busca redirigir la petición de usuario hacia otros destinos de manera forzada (redireccionar código).

* + 1. Interceptación

Es un tipo de amenaza que busca interceptar las comunicaciones de una red en la búsqueda de credenciales de acceso para luego suplantar al usuario real y ejecutar acciones para beneficio del atacante.

* + 1. taques de Fuerza Bruta

Es una amenaza cuyo objetivo es identificar o descifrar las credenciales de acceso real a los sistemas de información, para ello utilizan la técnica de ensayo error a través de bases de datos prestablecidas de credenciales de usuarios y contraseñas.

* + 1. Inadecuada seguridad

Se da por malas practicas en el manejo de recursos tecnológicos como la no actualización permanente del sistema operativo y aplicaciones, el uso de software ilegal o en algunos casos al recurrir a la activación no legal de aplicaciones lo que permite habilitar vulnerabilidades y generar huecos de seguridad que posteriormente serán explotados por un usuario no autorizado.

* + 1. Ingeniería social

Se basa en la utilización de las herramientas de comunicación digital en la búsqueda de información personal o sensible que puede ser utilizada como estrategia para la generación de cuentas de usuario y contraseñas de acceso, esta técnica utiliza medios como el teléfono, el correo electrónico, las redes sociales

Aunque con frecuencia el ataque se realiza de forma directa a una persona o empresa, también puede ser que tu equipo o dispositivo sea usado para atacar o amenazar a otros usuarios o empresas en el mundo

1. **Hacking ético**

Esta es una técnica que utiliza las mismas herramientas, técnicas, conocimientos y habilidades de un hacker para evaluar la seguridad de un sistema informático o de una red, pero de forma legal y ética, con el propósito de identificar y corregir posibles vulnerabilidades y corregirlas antes de que sean explotadas por hackers con propósitos malintencionados.

* 1. Propósito del Hacking ético

El propósito principal de un hacking ético es el buscar vulnerabilidades, explotarlas y buscar hackear los sistemas informáticos o redes de comunicaciones con el propósito de corregirlas esto permitirá que la organización sortee los eventos de ataques disminuyendo de esta manera la probabilidad de que hackers maliciosos puedan lograr su cometido de acceder a los recursos con un propósito mal intencionado.

* 1. Tipos de Hacking

Hay diferentes tipos de hackers con diferentes funciones, roles y propósitos de acuerdo con sus características se han ido especializando y creciendo lo que les ha permitió catalogarlos de la siguiente manera:

* + 1. Hackers Black Hat

Estos con conocidos como ciberdelincuentes que han logrado acceder o ingresar a sistemas informáticos y redes, su propósito es dañar y acceder a información de seguridad logrando con esto poner en posición de peligro al otro, dentro de esta categoría encontramos los crakers y phreakers, los primeros desarrollan software malicioso para modificar el software o hacer colapsar los servicios y aplicaciones contaminando servicios y redes y los segundos se especializan en la búsqueda y explotación de vulnerabilidades en las redes de telecomunicaciones en particular las de telefonía.

* + 1. Hackers White Hat

Son los llamados hackers éticos cuyo propósito es investigar y probar sistemas informáticos y redes en búsqueda de fallas de seguridad para notificarlas y lograr que de esta manera las organizaciones se protejan.

* + 1. Hackers Grey Hat

Estos hackers son mercaderes pues basan su ética de acuerdo con el lugar y las condiciones bajo las cuales trabajan. Es común que presten sus conocimientos y servicios para agencias de inteligencia, grandes empresas y entidades gubernamentales. Pueden llegar a divulgar información sensible bajo el establecimiento de precios.

* + 1. Hackers Newbies

Este tipo de hackers son muy peligros sobre todo de manera interna, son profesionales con uy poca experiencia que se empiezan dedicar al hacking ético pero por su inexperiencia y falta de conocimiento pueden provocar fallas y vulnerabilidades aprovechas por hackers con propósitos maliciosos. Son conocidos como los novatos del Hacking.

* + 1. Hacktivista

Son los hackers que se dedican a hacer hacking con fines y propósitos políticos, en los últimos años es donde mayor aumento de este tipo de hackers se ha dado en el mundo, el mayor ejemplo de este tipo de hacker es Anonymous quienes utilizan sus conocimientos y destrezas en la búsqueda de información que pueda ser divulgada de manera pública afectando negativamente algún gobierno o sector público o privado.

1. **Daño Informático**

Cuando hablamos de daños informáticos debemos remitirnos a la legislación de nuestro país, un daño informático es considerado como un delito de acuerdo con la ley 1273 de 2009 por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos".

Dentro de la tipificación de los delitos informáticos en Colombia se menciona en el articulo 269D de la ley 1273 lo siguiente:

DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Como lo menciona el articulo en la ley los tipos de daños informático son los siguientes:

* Destrucción de datos
* Dañar
* Borrar
* Deterioro
* Alteración
  1. Delito Informático

Se considera un delito informático toda acción ilegal realizadas como los delitos tradicionales o tipificados en el código penal colombiano que involucran el uso de la tecnología o el internet para desarrollar dicha acción.

* 1. Tipificación de los delitos informáticos

En la ley 1273 de 2009 se tipifican los delitos, los cuales se encuentran contemplado de la siguiente manera:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

* Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
* Por servidor público en ejercicio de sus funciones
* Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
* Revelando o dando a conocer el contenido de la información en perjuicio de otro.
* Obteniendo provecho para si o para un tercero.
* Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
* Utilizando como instrumento a un tercero de buena fe.
* Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

1. **Ciberseguridad**
   1. Definición

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Cano, J. (2011).

* 1. Generalidades

En los últimos años el concepto de ciberseguridad se ha convertido en un estándar y en una necesidad en todas las organizaciones puesto que cada vez más y con mayor frecuencia se recurre al uso de las tecnologías de la información y las comunicaciones para apalancar los procesos operativos y core del negocio, el desarrollo y evolución de la tecnología nos lleva a hacer uso de servicios como internet, la interconexión entre sedes y con mayor frecuencia la utilización de tecnologías de computación en la nube lo que necesariamente obliga a las empresas a proteger sus recursos y su información del acceso no autorizado y de todas las posibles amenazas de las cuales pueden ser víctimas.

Protegerse de los peligros de la actual coyuntura tecnológica nos lleva a diseñar y adoptar una serie de procesos que nos posibiliten la protección de sus activos, recursos e información y para ello se recomienda la aplicación de las siguientes fases:

* + 1. Prevención

Esta es la primera fase que ayudara de manera significativa en la disminución de los riesgos, actuar de manera temprana implica conocer nuestros activos o recursos tecnológicos usados en la organización y realizar un análisis de las posibles amenazas y la forma en que podríamos prevenirlas o contrarrestarlas, en esta fase es de gran importancia la concienciación que se debe de hacer en todos los miembros de la organización, prepararlos, capacitarlos y crearles conciencia permitirá que se cometen un número menor de errores que muchas veces por desconocimiento generan vulnerabilidades y riesgos que pueden ser prevenidos y detectados con anterioridad.

* + 1. Localización:

Luego de prevenir debemos concentrarnos en la adquisición e implementación de una serie de herramientas tecnológicas que nos permitan en caso de presentarse algún tipo de incidente poder localizar su fuente y afectación a fin de tomar las acciones correctivas a que dieran lugar.

Esto se logra cuando las medidas y herramientas empleadas están haciendo un constante monitoreo y gestión sobre los recursos tecnológicos, normalmente cuando se detectan los incidentes estos ya han ocurrido muchos días antes ya que cada vez los atacantes utilizan más herramientas y estrategias avanzadas que dificultan su detección, de ahí la importancia de una constante monitorización sobre sus recursos y servicios tecnológicos.

* + 1. Reacción:

Una vez se detecte una posible amenaza se debe realizar una reacción inmediata que permita su mitigación, para esto se recomienda seguir los siguientes pasos:

* Desconectar los activos de la red que están siendo afectados
* Actualizar los sistemas de protección implementados como antivirus, antimalware, anti spyware, entre otras estrategias implementadas en la organización.
* Realizar un análisis exhaustivo sobre los sistemas o servicios afectados a fin de detectar el origen y afectación
* Cambiar todas las contraseñas
* Realizar una limpieza profunda de los recursos tecnológicos con las herramientas con que cuente la organización.

Con la evolución de la tecnología, los avances y el desarrollo tecnológico actual se ha masificado el uso de internet y el uso de distintas plataformas y servicios en la nube, dese acceso a servicios simples como las páginas de contenido web, envío y recepción de documentos, compras y pagos en línea hace que los cibernautas o usuarios de internet y las redes de datos se vean gravemente comprometidos de no contar con las protecciones y herramientas adecuadas lo que hiso que naciera la seguridad informática, la seguridad de la información y recientemente la Ciberseguridad con la inclusión de la norma ISO 27032.

En este sentido la Organización Internacional de Estándares crea la nueva norma ISO 27032 como complemento a la serie de normas ISO 27001 con el objetivo de proteger las transacciones en línea, es decir garantizar la seguridad en el ciberespacio.

La norma ISO 27032 como se mencionó es un complemento que trabaja de la mano con los conceptos de seguridad informática, seguridad en la red, seguridad en Internet, ciberdefensa, cibercrimen tal como se muestra a continuación.

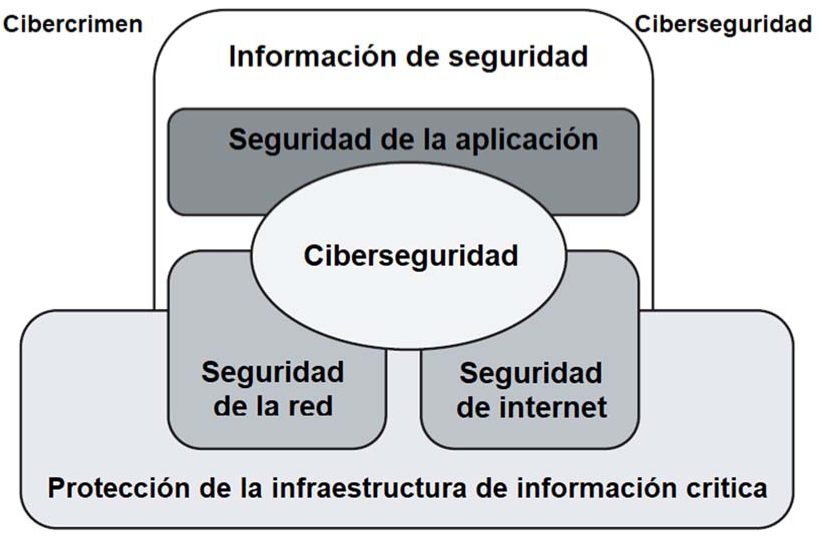


imagen 11: Relación entre Ciberseguridad y demás ámbitos de la seguridad. Tomado de NTC ISO\_IEC\_27032

En términos generales la implementación de la norma ISO 27032 y de la ciberseguridad en una organización se puede centrar en 4 áreas especificas de trabajo las cuales son:

* Seguridad de la información: Protección de los datos en cualquier medio frente a las amenazas
* Seguridad de las redes: se centra en la protección de los mecanismos de autenticación y posterior asignación de roles y permisos para acceder a una red o dispositivo.
* Seguridad en Internet: enfoca en identificar y prevenir todas las amenazas que afectan el internet.
* Protección de las infraestructuras criticas: enfocada en la protección de los dispositivos y/o servicios críticos.

La ciberseguridad se enfoca en la identificación y gestión de los riesgos en 4 enfoques principales:

* Prevención: se deben de implementar controles, contramedidas y medidas de limiten o mitiguen al máximo los impactos ocasionados por posibles eventos de ciberseguridad.
* Protección y Detección: se deben implementar controles para la monitorización y gestión de eventos de seguridad con el fin de detectarlos, corregirlos y protegerse antes los eventos detectados. (Correlacionador de eventos).
* Respuesta y comunicación: se debe preparar la organización para que responda a eventos de ciberseguridad que permita mitigarlos una vez se materialicen.
* Recuperación y aprendizaje: se deben de establecer los mecanismos necesarios para recuperar o restaurar servicios y sistemas que se hallan afectado por algún evento y definirse los procedimientos y políticas para reducir la probabilidad de que se vuelvan a presentar.

Seguido de lo anterior es indispensable desarrollar también una metodología interna para la implementación de la norma. Para dicho propósito, es recomendable dividir en al menos cuatro fases este proceso:

Para una correcta implementación de la ciberseguridad apalancada en el estándar ISO 27032, se puede definir una metodología interna que permita centrar el proceso en 4 áreas de trabajo:

* 1. Fases de implementación de ciberseguridad

* + 1. Entendimiento de la organización.

Esta primera fase consiste en el reconocimiento y entendimiento de la organización para conocer su funcionamiento, servicios, aplicaciones, su funcionamiento y su relación con el ciberespacio, algunas de las actividades de esta fase son las siguientes:

* Revisión e inventario de productos y servicios (Identificación de activos)
* Revisión de los marcos de trabajo de ciberseguridad utilizados o por utilizar en la organización
* Recopilar, revisar y analizar la documentación de seguridad.
* Identificar los procesos y determinar los flujos de información presentes
* Identificar si existen o no medidas técnicas de seguridad implementadas.
  + 1. Análisis de Riesgos.

Se debe de identificar y evaluar a finde determinar la gestión de los riesgos, esto nos permitirá definir las medidas y controles de seguridad a implementar de acuerdo con el entendimiento y alineamiento de los objetivos institucionales de la empresa.

En esta fase se hace la valoración y evaluación de los riesgos considerando:

* Activos críticos
* Amenazas
* Vulnerabilidades
* Impacto y riesgo
* Responsabilidades
  + 1. Plan de acción

Con base al trabajo realizado en las fases anteriores en esta fase se deben de priorizar las medidas y controles a implementarse para la consecución de los objetivos de alineamiento de la norma ISO 27032 y los objetivos o exigencias de la empresa. Dentro de las acciones a desarrollarse estas deberán estar distribuidas en diferentes niveles de la organización dentro de las cuales encontramos las siguientes.

* Políticas de seguridad y ciberseguridad
* Identificación y categorización de roles
* Métodos de implementación
* Procesos afectados
* Controles o medidas se seguridad
  + 1. Implementación

Es la última etapa y la que mas tiempo y esfuerzo demanda puesto que es en la que se plasmaran implementaran todas las acciones previamente definidas en la etapa anterior, acá es importante mencionar que la norma ISO 27032 siempre recomienda o centra su aplicación en el ser proactivo y hacer mayor énfasis en los controles y mecanismos de prevención sobre todo con los procesos que hacen uso del internet y el ciberespacio.

Se deben implementar controles que tengan en cuenta el nivel de madurez en la seguridad existente y que debe incluir los siguientes aspectos.

* Existencia o no de política de seguridad
* Procedimientos de seguridad en todo el ciclo de vida del desarrollo de sistemas.
* Marcos existentes y adoptar uno para el intercambio de información
* Planes de capacitación y concienciación a todo el personal.
* metodologías de análisis y valuación de riesgos
* Monitoreo y gestión
* Gestión de incidentes.
* Controles a nivel de aplicación
* Controles a nivel de servidores
* Controles para los usuarios finales.
* Controles contra ataques de ingeniería social.

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

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

1. **MATERIAL COMPLEMENTARIO:**

|  |  |  |
| --- | --- | --- |
| **Referencia APA del Material** | **Tipo de material**  **(Video, capítulo de libro, articulo, otro)** | **Enlace del Recurso o**  **Archivo del documento o material** |
| Avance Jurídico Casa Editorial Ltda. (2023, August 17). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY\_1273\_2009]. Senado de la República de Colombia. Recuperado desde http://www.secretariasenado.gov.co/senado/basedoc/ley\_1273\_2009.html | Artículo publicado en el diario oficial del senado de la república. | http://www.secretariasenado.gov.co/senado/basedoc/ley\_1273\_2009.html |
| Tecnologías de la información. técnicas de seguridad. directrices para ciberseguridad. (2023, September 11). Retrieved from https://tienda.icontec.org/gp-tecnologias-de-la-informacion-tecnicas-de-seguridad-directrices-para-ciberseguridad-gtc-iso-iec27032-2020.html | Sitio donde se puede comprar la norma técnica colombiana | https://tienda.icontec.org/gp-tecnologias-de-la-informacion-tecnicas-de-seguridad-directrices-para-ciberseguridad-gtc-iso-iec27032-2020.html |
|  |  |  |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| **TERMINO** | **SIGNIFICADO** |
| Activo | El término de activo de información se relaciona con todos esos elementos tecnológicos o relacionados con la tecnología que la organización utiliza para el cumplimiento de sus metas o core del negocio. Según la norma ISO/IEC 27001 se entiende como activo todo aquello que es importante y que la organización valora por lo tanto debe de protegerse |
| Riesgo | Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque sobre un recurso o servicio tecnológico. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza. |
| SGSI | Sistema de gestión de Seguridad de la Información |
| Amenaza | Cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. |
| Vulnerabilidad | Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma. |
| ISO 27001 | Estándar de Organización de estándares internacionales relacionado con la seguridad de la información. |
| ISO 27032 | GTC-ISO/IEC 27032, Tecnologías de la información, Técnicas de seguridad. directrices para ciberseguridad. |
| Alcance (Inglés: Scope). | Ámbito de la organización que queda sometido al SGSI |
| Amenaza (Inglés:Threat). | Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. |
| Ataque (Inglés: Attack). | Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo. |
| Auditoría  (Inglés: Audit). | Proceso sistemático, independiente y documentado para obtener evidencias de auditoriía y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría. |
| Autenticación  (Inglés: Authentication). | Provisión de una garantía de que una característica afirmada por una entidad es correcta. |
| Confidencialidad  (Inglés: Confidentiality). | Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. |
| Control  Medida por la que se modifica el riesgo. | [Fuente: ISO Guide 73:2009] Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguarda o contramedida son utilizados frecuentemente como sinónimos de control. |
| Disponibilidad  (Inglés: Availability) | Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. |
| Evaluación de riesgos  (Inglés: Risk assessment). | Proceso global de identificación, análisis y estimación de riesgos. [Fuente: ISO Guide 73:2009] |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

* Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. SISTEMAS (ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS), 119, 4-7.
* Calder, A. (2018). NIST Cybersecurity Framework: Una guía de bolsillo . IT Governance Publishing Ltd.
* NIST Framework for Improving Critical Infrastructure Cybersecurity https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
* Soriano, M. (2014). Seguridad en redes y seguridad de la información. Obtenido de http://improvet. cvut. cz/project/download/C2ES/Seguridad\_de\_Red\_e\_Informacion. pdf.
* Magerit v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Disponible en: https://www.ccn-cert.cni.es/publico/ herramientas/Pilar-5.4.1/web/magerit/Libro\_I\_metodo.pdf.
* Seguridad 7”A”Metodología NIST SP 800-30 (National Institute of Standards and Technology), Disponible en: http://seguridades7a.blogspot.com/p/ nist-sp-800-30.html.
* M. Juan. (2009), Análisis de Riesgos de Seguridad, [On line]. Disponible en: http://oa.upm.es/1646/1/ PFC\_JUAN\_MANUEL\_MATALOBOS\_VEIGAa.pdf
* Avance Jurídico Casa Editorial Ltda. (2023, August 17). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY\_1273\_2009]. Senado de la República de Colombia. Retrieved from <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>
* Tecnologías de la información. técnicas de seguridad. directrices para ciberseguridad. (2023, September 11). Retrieved from https://tienda.icontec.org/gp-tecnologias-de-la-informacion-tecnicas-de-seguridad-directrices-para-ciberseguridad-gtc-iso-iec27032-2020.html

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia**  ***(Para el SENA indicar Regional y Centro de Formación)*** | **Fecha** |
| **Autor (es)** | Henry Eduardo Bastidas Paruma | Instructor | Regional Cauca, Centro de teleinformática y producción industrial | Septiembre 11 de 2023 |
|  |  |  |  |

1. **CONTROL DE CAMBIOS**

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

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