Introduccion a la seguridad 2

Informacion:

Es un grupo de datos ya procesados y ordenados,que sirven para construir un mensaje que cambia el estado de conocimiento del sujeto o sistema que lo recibe.
La palabra informacion deriva del latin que significa “dar forma mente”,”disciplinar”,instruir”,”enseñar”.

Característica de la información

Crítica:Es indispensable para la operación de la organización.

Valiosa:Es un activo apreciado por la organización y sus operaciones.

Sensitiva:Debe de ser conocida por las personas autorizadas.

Triangulo ID

Es el triángulo de la **seguridad de la información**, formado por:

Confidencialidad: Solo usuarios autorizados acceden a la información.

Integridad: Los datos no deben ser alterados de forma no autorizada.

Disponibilidad: La información debe estar accesible cuando se necesite.

Seguridad:

Proviene del latin securitas que deriva cuidado,sin precaución,sin temor a preocuparse qué significa libre de cualquier peligro o daño.
Se considera como un estado mental que produce en los individuos un particular sentimiento de que se está fuera o alejado de todo peligro ante cualquier circunstancia.

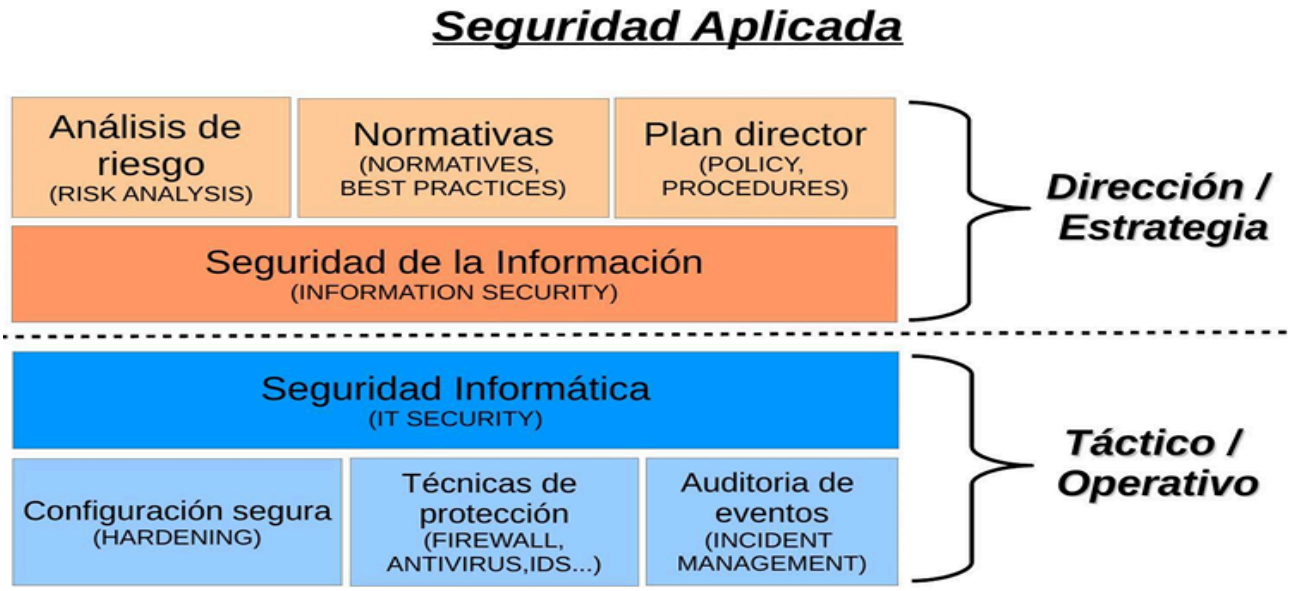
Seguridad de la informacion:

Es la disciplina que nos habla de los riesgos,de las amenazas,de los análisis de escenarios,de las buenas prácticas y esquemas normativos,que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación,uso,almacenamiento,transmisión,recuperación y disposición final de la información.

Seguridad informatica:

Se encarga de las implementaciones técnicas de la protección de la información ,el despliegue de las tecnologías antivirus,firewalls ,detección de intrusos,detección de anomalías,correlación de eventos ,atención de incidentes,entre otros elementos,que articulados con prácticas del gobierno de tecnologia de informacion,establecen la forma de actuar y asegurar las situaciones fallas parciales o totales,cuando la

información es el activo que se encuentra en riesgo.



Seguridad de la información

Politica de seguridad:

Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que estan expuestos.Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

Plan director de seguridad:

Proyecto consistente en la definición y priorización de una conjunto de medidas en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables.

Analisis de riesgos:

Es un proceso que comprende la identificación de activos de información,sus vulnerabilidades y las amenazas a los que se encuentran expuestos ,así como la probabilidad de ocurrencia y el

impacto de las misma,a fin de determinar los controles adecuados para tratar el riesgo.

Incidentes de seguridad

Son violaciones de seguridad que ocasionan destrucción acceso no autorizado,pérdida o alteración de datos personales cuando están siendo transmitidos están almacenados o son objeto de otros tratamientos.

Origen de los incidente:

- Accidente
- Interno(miembros de la organización)
- Ciberataque:Intento deliberado de obtener acceso a un sistema informatico sin autorizacion en base al uso de diferentes tecnicas y vulnerabilidades para la realizacion de actividades con fines maliciosos,como el robo de informacion,extorsion del propietario o simplemente daños al sistema.
- Términos relevantes:riesgo,amenaza,no repudio,vulnerabilidades y anonimato.

Las causas de la inseguridad

Estado de inseguridad activo:

La falta de conocimiento del usuario acerca de las funciones del sistema,algunas de las cuales pueden ser dañinas para las seguridad del mismo.Este estado se encuentra directamente relacionado con la acción humana que genera al sistema una condición que puede ser utilizada por un atacante para generar un daño.

- Activar servicios de red que el usuario no necesita.
- Abrir un archivo adjunto malicioso.
- Proporcionar información confidencial

Estado de inseguridad pasivo:

La falta de conocimiento de las medidas de seguridad disponibles.Este escenario no está vinculado a la actividad humana,sino que está

constituido por condiciones preexistentes que pueden ser utilizadas por un atacante para generar un daño.

- Cuando el administrador o usuario de un sistema no conocen los dispositivos de seguridad con los que cuentan.
- Errores en el código de un programa.
- Permisos incorrectos o configuración desactualizada de un sistema.
- Defectos de hardware.

Requisitos funcionales para la seguridad

- Auditoría de seguridad:registro de actividades.
- Soporte de cifrado:uso de criptografía para la protección de datos.
- Gestión de seguridad:gestión de perfiles de usuario y niveles de acceso vinculados a los mismos.
- Privacidad:soporte del anonimato de los usuario.
- Autodefensa:controles para fallar de manera contenida o prevista.
- Control de acceso:manejo de la cantidad y tiempo de las sesiones,concurrencia e información sobre sesiones previas.
- Rutas o canales fiables:mecanismos que permitan confiar en los recursos accedidos como los certificados.

Seguridad logica

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo.

- Controles de acceso
- Identificacion y autenticacion
- Roles
- Transacciones
- Limitaciones a los servicios
- Modalidad de acceso
- Ubicacion de acceso interno
    - ☐ Palabras claves(Passwords)

- ☐ Cifrado
- ☐ Listas de control de accesos
- ☐ Límites sobre la interfaz de usuario
- ☐ Etiquetas de seguridad
- ☐ Palabras claves(Passwords)
- ☐ Cifrado

- Control de acceso externo:
  - ☐ Dispositivos de control de puertos
  - ☐ Firewalls o puertas de seguridad
  - ☐ Acceso de personal contratado o consultores
  - ☐ Acceso públicos

- Administración:
  - ☐ Administración del personal y usuario
  - ☐ Organización del personal

Practicas de seguridad logica en moviles

- Usar contraseñas robustas y bloqueo automático.
- Realizar copias de seguridad periódicas.
- Instalar software sólo de fuentes oficiales.
- Utilizar software solo con acceso legal a sus funcionalidades.
- Considerar el uso de software de seguimiento,borrado de datos y/o bloqueo remoto.
- Evitar o restringir conexiones a redes públicas o no confiables.
- Deshabilitar sistemas de bluetooth,NFC y otras tecnologías inalámbricas cuando no se requiera el uso de los mismos en dispositivos confiables.
- En dispositivos con conexión de datos móviles tener el PIN activado y su el PUK e IMEI memorizado

Rastreo y gestion remota de dispositivos

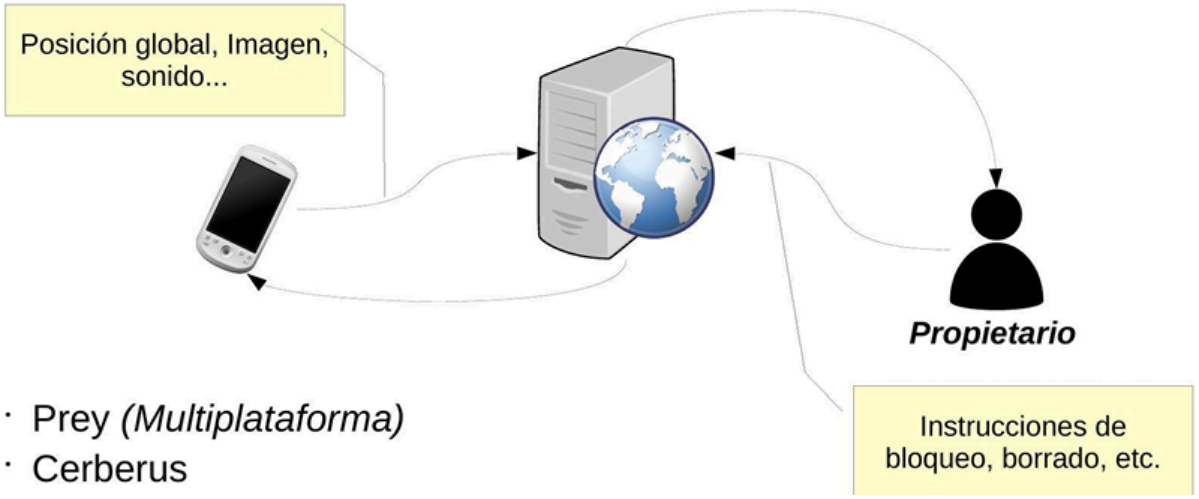
Este tipo de software permite realizar operaciones de forma remota sobre el equipo permitiendo el siguiente tipo de acciones:

- Rastreo del dispositivo
- Borrado de datos
- Bloqueo del dispositivo
- Obtención de información del medio(grabación de audio ,video,etc).

Son aplicaciones particularmente útiles antes situaciones de perdida y robo.
Su funcionalidad suele estar limitada por la conectividad del equipo.

Rastreo y gestion remota

- Prey(Multiplataforma)
- Cerberus
- Avast Anti-Theft
- Android(Ajustes / Seguridad/ Administradores del dispositivo)
- Iphone(¡Cloud.com/ Find My Iphone)



Copias de seguridad

Una política de copia de seguridad es un documento que define las reglas y procedimientos para la creación,almacenamiento y gestión de

las copias de seguridad de datos en una organización.Esta debe ser revisada periódicamente para asegurar que se ajusta a las necesidades de la organización.
La política definirá frecuencia y modalidad de las copias,esto último puede ajustarse a los siguientes tipos:

- Copia total:Hace una copia completa de todos los datos seleccionados, sin importar si cambiaron o no.
- Copia diferencial:Copia solo los archivos que cambiaron desde la **última copia total**.
- Copia incremental:Copia solo los archivos que cambiaron desde la **última copia (sea total o incremental)**.

La definición de la política y su ejecución debe considerar los siguientes puntos:

- Soporte de la copia(Cinta,discos,memorias,cloud,etc)
- Pruebas de restauraciones periódicas.
- Control de acceso a las copias
- Rotación de medios y período de retención
- Almacenamiento y traslados
- Eliminación y reutilización de soportes

Seguridad logica

Estos son otros elementos comunes en el manejo de la seguridad de sistemas:

- Firewalls: Son dispositivos o software que filtran el tráfico de red.Funcionan como un "portero" entre una red confiable (como tu computadora o red interna) y una no confiable (como Internet).Bloquean o permiten paquetes de datos según reglas predefinidas.
- Firewalls personales:Son firewalls instalados en una sola computadora.Protegen el equipo del tráfico no autorizado o sospechoso.
- Honeypots:Sistema trampa diseñado para atraer atacantes y analizar su comportamiento.

- Honeynets:Conjunto de honeypots conectados entre sí simulando una red real.
- Padded cells:Entorno seguro donde, una vez detectado, se traslada al atacante para monitorearlo sin riesgo al sistema real.
- Verificadores de integridad:Herramientas que monitorizan si archivos críticos han sido modificados.
- IDS (Intrusion Detection System):Sistema que detecta comportamientos anómalos o sospechosos en una red o sistema. No actúa automáticamente, solo avisa (genera alertas). Puede ser basado en firmas (como un antivirus) o en comportamiento.
- IPS (Intrusion Protection System):Similar al IDS, pero va un paso más allá: no solo detecta, también bloquea el tráfico malicioso en tiempo real.Actúa como defensa activa. Suele ir integrado con firewalls o sistemas de red.
- Antivirus:Programa que detecta, bloquea y elimina malware como virus, gusanos, troyanos, etc. Funciona principalmente a través de bases de firmas y análisis heurístico. Se enfoca en el nivel de archivos y procesos.
- WAF(Web Application Firewall): es un tipo de firewall que protege las aplicaciones web filtrando, monitoreando y bloqueando tráfico HTTP(S) malicioso hacia y desde una aplicación web. Su función principal es prevenir ataques comunes como Inyección SQL,Cross-Site Scripting (XSS),Cross-Site Request Forgery (CSRF),Fuerza bruta,File inclusion.

Referencia VPN

Una estructura de red que con soporte logico que permite el tráfico de información privada sobre una infraestructura de red pública mediante el uso de criptografía.
Protocolos:

- IPSec
- SSL/TLS
- PPTP,L2TP

Seguridad fisica

Tipo de desastres:

- Desastres naturales,incendios accidentales tormentas e inundaciones
- Disturbios,sabotajes internos y externos deliberados.
- Amenazas ocasionadas por el nombre.

Acciones hostiles:

- Robo
- Fraude
- Sabotaje

Control de accesos:

- Utilizacion de guardias
- Utilizacion de detectores metales
- Utilizacion de sistemas biometricos
- Verificacion automatica de firmas(VAF)
- Seguridad con animales
- Proteccion electronica

Practicas de seguridad fisica en moviles

- Evitar o restringir la manipulación del dispositivo en zonas públicas.
- No transportar el dispositivo en contenedores que puedan ser visibles a terceros .
- Utilizar contenedores de transporte que reduzcan la fuerza ante impactos.
- Utilizar contenedores de transporte que protejan al dispositivo del contacto con líquidos.

Impacto en la organizacion

- Pérdida de datos:puede afectar la reputación,la productividad y la rentabilidad de la organización.

- Robo de identidad:puede afectar a los clientes y empleados de la organización.
- Interrupción del negocio:puede causar daños económicos y afectar la imagen de la organización.
- Daño a la reputación:puede afectar la confianza de los clientes y socios de la organización.

  Factores a considerar en el impacto de la seguridad en la organización y sus procesos:

- Cambios en lo que respecta a los riesgos para la seguridad a traves del tiempo.
- Políticas de seguridad corporativa.
- Evaluación y tratamiento del riesgo.
- Políticas de control de accesos.
- Gestión de la continuidad del negocio.
- Procedimientos de cumplimiento y de las operaciones.
- Manejo de las comunicaciones y de las operaciones.
- Administración de los incidentes en seguridad de la información.
- Protocolos para la gestión de los activos.
- Adquisición,desarrollo y mantenimiento de los sistemas de información.
- Seguridad física y ambiental.
- Organización de la seguridad de la información.
- Integración de la seguridad de la información.