**UNIDAD 1 – HIPER RESUMEN**

**INFORMACION**

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.

Características;

* Critica; es indispensable para la operación de la organización.
* Valiosa; es un activo apreciado por la organización y sus operadores.
* Sensitiva; debe de ser conocida por las personas autorizadas

Triangulo de *sensitivo*;

* Confidencialidad
* Disponibilidad
* Integridad; no se modificó ni se rompió, confianza

**SEGURIDAD DE LA INFORMACION**

Disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas practicas 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.

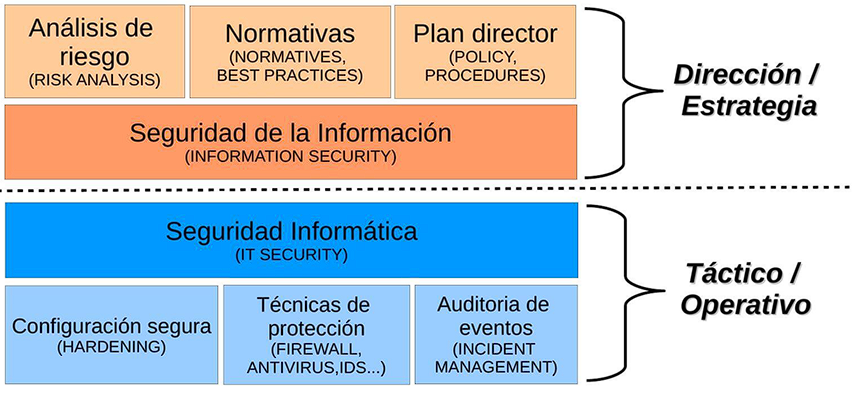
Política de seguridad; medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos.

Plan director de seguridad; definición y priorización de un 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, a partir de un análisis de la situación inicial

Análisis de riesgos; proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos.

**SEGURIDAD INFORMATICA**

Se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías, antivirus, firewalls, detección de intrusos, de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.



**INCIDENTES DE SEGURIDAD**

Ciberataque; intento deliberado de obtener acceso a un sistema informático sin autorización en base al uso de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos.

Intrusión; acción provocada por un ataque o usuario malintencionado, que se aprovecha de una vulnerabilidad en el sistema para conseguir acceder a un área o dispositivos sin autorización.

Riesgos;

Amenazas;

No repudio;

Vulnerabilidades;

Anonimato;

**CAUSAS DE INSEGURIDAD**

Estado de inseguridad activo; falta de conocimiento del usuario de las funciones del sistema (activar servicios de red que el usuario no necesita, abrir un archivo adjunto malicioso, proporcionar información confidencial)

Estado de inseguridad pasivo; falta de conocimiento de las medidas de seguridad disponibles. (cuando el admin no conoce los dispositivos de seguridad, errores en el código, permisos incorrectos o configuración desactualizada, defectos de hardware)

**REQUISITOS FUNCIONALES PARA LA SEGURIDAD**

* Auditoria de seguridad
* Soporte de cifrado
* Gestión de seguridad
* Privacidad
* Autodefensa
* Control de acceso
* Rutas o canales fiables

**HASH**

Método no reversible para generar un valor que represente de manera casi univoca un dato.

**SEGURIDAD LOGICA**

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

* Controles de acceso
* Identificación y autenticación
* Roles
* Transacciones
* Limitaciones a los servicios -> en base a todos los puntos posteriores
* Modalidad de acceso
* Ubicación y horario
* Control de acceso interno
  + Palabras claves
  + Cifrado
  + Listas de control de accesos
  + Límites sobre la interfaz de usuario
  + Etiquetas de seguridad
* Firewalls y firewalls personales.
* Escaners de vulnerabilidad
* Honeypots, honeynets, padded cells
* Verificadores de integridad
* IDS, IPS
* Antivirus
* WAF

**PRACTICAS DE SEGURIDAD LOGICA EN MOVILES**

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

**BYOD**

Política empresarial para el uso de dispositivos tecnológicos que se caracterizan por permitir a los empleados el uso de sus propios dispositivos personales para el trabajo, así como también el acceso desde los mismos a las redes corporativas, aceptando su uso compartido para las tareas profesionales como para las personales.

**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 de dispositivos
* Obtención de información del medio

Son aplicaciones particularmente útiles ante las situaciones de perdida y robo. Su funcionalidad suele estar limitada por la conectividad del equipo. (Prey, Cerberus, Avast anti theft, Android, Iphone)

**COPIAS DE SEGURIDAD**

Una política de copias 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. Este debe ser revisada y actualizada periódicamente para asegurar que se ajusta a las necesidades de la organización

Frecuencia y modalidad de copias: copia total, copia diferencial, copia incremental (nuevos datos)

La política debe considerar:

* Soporte de la copia (discos, memorias, nube)
* Pruebas de restauración periódicas (practica re piola)
* Control de acceso a las copias
* Rotación de medios y periodo de retención
* Almacenamiento y traslados
* Eliminación y reutilización de soportes

**VPN**

Estructura de red que con soporte lógico que permite el tráfico de información privada sobre una infraestructura de red publica mediante el uso de criptografía

Protocolos; IPSec, SSSL / TLS, PPTP, L2TP

**SEGURIDAD FISICA**

Consiste en mecanismos destinados a proteger físicamente cualquier recurso del sistema de amenazas producidas tanto por el hombre como por la naturaleza; en general serán prevención y detección

Tipos de desastres

* Desastres naturales
* Disturbios, sabotajes internos y externos deliberados
* Amenazas

Acciones hostiles

Control de accesos

**IMPACTO EN LA ORGANIZACIÓN**

* Perdida de datos
* Robo de identidad
* Interrupción del negocio
* Daño a la reputación