UNIDAD 1 – INTRODUCCION A LA SEGURIDAD

Información

Cuando algo se expone cambia el estado de algo. Todo lo que se considere información modifica lo que la persona conoce.

Características

- **Critica:** Si no se conoce, no se puede realizar la acción.
- **Valiosa:** La importancia que se le da, se puede prescindir de dicha información y así y todo, realizar las operaciones.
- **Sensitiva:** Debe ser conocida por las personas autorizadas. Quien debe conocer dicha información.

Dimensiones de la Seguridad de la información

La seguridad de la información se articula sobre tres dimensiones, que son los pilares sobre los que aplicar las medidas de protección de nuestra información:

- **Integridad**: hace referencia a que la información sea correcta y esté libre de modificaciones y errores.
- **Disponibilidad**: hace referencia a que la información esté disponible.
- **Confidencialidad**: implica que la información es accesible solo por el personal autorizado. Conocido como “need-to-know”

La información debe estar bien clasificada.
La información de la persona suele ser sensible (datos personales, datos de origen racial, datos de condenas penales, etc), esta no debe ser expuesta.
Se debe saber que información se tendrá en el sistema para saber que métodos y costos manejar.
La adopción de un determinado control para mejorar la seguridad en una dimensión puede afectar de forma negativa o positiva a otra de las dimensiones, por ello hay que saber que dimensión es mas importante para nuestro sistema. Es decir, Cuanto más se aplique en uno de ellos (confidencialidad, integridad o disponibilidad), menor dominio tendrá sobre el resto

Selección de Salvaguardas

Medidas necesarias para proteger la información de nuestro negocio. Para ello se deben tener en cuenta los siguientes aspectos:

- Determinar la importancia de la información que manejamos
- Identificar, clasificar y valorar la información según las dimensiones de seguridad
- Conocer la naturaleza de los controles que se pueden implantar
- Costo de las medidas

Clasificación de la información

- **Confidencial:** información especialmente sensible para la organización. Acceso restringido
- **Interna:** información propia de la empresa, accesible para todos sus empleados
- **Publica:** Cualquier material de la empresa sin restricciones de difusión

Tipología de selección de controles

- **Técnica:** medidas de carácter tecnológico dentro del ámbito de la seguridad. (Antivirus, cortafuegos, sistemas de copias de seguridad)
- **Organizativa:** medidas que se centran en la mejora de la seguridad teniendo en cuenta a las personas. (formación de seguridad, responsables)
- **Física:** medidas físicas para proteger la organización. (acondicionar sala de servidores frente a riesgos de incendios)

Seguridad de la Información

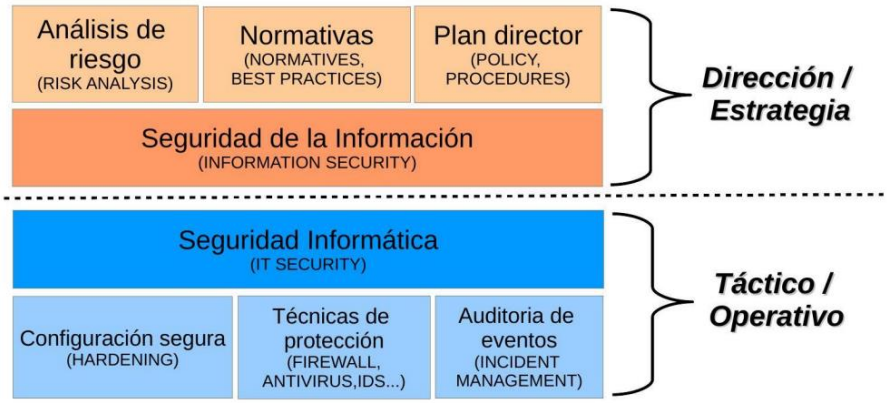
Disciplina que habla de los riesgos, amenazas, análisis de escenarios, buenas practicas y esquemas normativos que nos exigen los niveles de aseguramiento de procesos y tecnologías.

- **Política de seguridad:** medidas o decisiones que una empresa toma respecto de la seguridad de sus sistemas informáticos. Documento con el cual establece las normas de seguridad.
- **Plan director de seguridad:** proyecto con conjunto de medidas en materia de seguridad con el objetivo de reducir los riesgos a los que está expuesta la empresa.
- **Análisis de riesgo:** proceso que evalúa la identificación de activos de información, sus vulnerabilidades y las amenazas a las que está expuesta y prioriza las medidas que se tomen para evitarlos.

Seguridad informática

Se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, entre otros, que articulados con prácticas de gobierno de tecnología de información, establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales.
El estado de seguridad de una aplicación es dinámico. Este se debe ir modificando ya que al paso del tiempo comienzan las vulnerabilidades.

Seguridad Aplicada



Incidentes de seguridad

Violaciones de la seguridad que ocasionan la destrucción, acceso no deseado, pérdida o alteración de la información. Es cualquier evento no esperado. Estos se dividen en 3 tipos de incidentes:

- **Accidente:** No necesariamente fue atacado, sino que por accidente tuvo filtración de datos.
- **Ciberataque:** Lo realiza un agente externo con planificación previa. Es el intento deliberado de obtener acceso a información por medio de uso de diferentes técnicas y vulnerabilidades. Refieren a información específica.
- **Intrusión:** Acción realizada por un atacante o usuario malintencionado con el fin de tener acceso a áreas no correspondidas.

Términos Importantes

- **Riesgos:** Es algo negativo, probabilidad de que ocurra algo no deseable. Se prevé con un análisis de riesgos.
- **Amenazas:** Algo que potencialmente puede generar un daño al sistema. Algo externo. Aquella situación de daño cuyo riesgo de producirse es significativo.
- **Vulnerabilidad:** Cosas que pueden derivar en un daño: bug, una falla, etc. Es un problema interno, se puede realizar algo al respecto frente a cierto riesgo.
- **No Repudio:** Cuando se recibe un mensaje no solo es necesario poder identificar de forma univoca al remitente, sino que este asuma todas las responsabilidades derivadas de la información que haya podido enviar. Es fundamental impedir que el emisor pueda repudiar un mensaje, es decir, negar su autoría en el. Como demostrar que una persona realizo x acción. Diferentes métodos que lo verifiquen. Ejemplo: una transacción de que fue realizada frente a una compra virtual.
- **Anonimato:** Concepto opuesto al *No Repudio*. Se desconoce la fuente. Identificar a la persona implica un costo. Se cambia la disponibilidad de la información.
- **Autentificación:** Asociado a la comprobación del origen e integridad de la información. Garantizar el correcto funcionamiento de sistema operativo conlleva a poder verificar de forma fiable la autenticidad de los distintos elementos que interactúan en sí, la información que se recibe, envía y almacena, los usuarios que acceden al mismo y los dispositivos que se comunican con él.
- **Control de Acceso a los Datos:** Acceder a la información solo por agentes autorizados. Utilizar métodos de restricción de acceso a dicha información.

- **Seguridad de los Canales de Comunicación:** Establecer mecanismos de protección de la información ya que los canales suelen ser muy vulnerables.
- **Seguridad Física:** Constituyen lo que se relaciona con la salvaguarda de los soportes físicos de la información. Análisis contra incendios, sobrecargas eléctricas, etc.

Contenedores de Información

Los sistemas aislados poseen mayor seguridad. Suelen utilizar tecnología vieja ya que resulta más difícil de manipular.

- **Sistemas Aislados:** Son los que no tienen acceso a ningún tipo de red. Conllevan protocolos de gestión de los privilegios de cada usuario.
- **Sistemas Interconectados:** La mayoría de los elementos que nos rodean hoy en día (celulares, PC, Smart tv, etc.). Todo aquello que tiene acceso a internet.

Las Causas de la Inseguridad

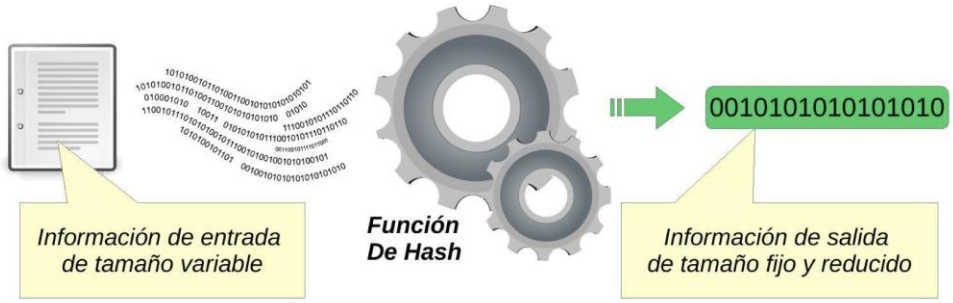
- **Estado Inseguridad Activo:** Cuando por una acción tomada, se encuentra en estado inseguro. Por ejemplo: Apagar el antivirus.
- **Estado Inseguridad Pasivo:** Cuando se encuentra inseguro por no haber realizado una acción. Por ejemplo: Olvidar de activar el antivirus.

Requisitos Funcionales para la Inseguridad

- **Auditoria de Seguridad:** Registro de actividades. Poder reproducir que ocurrió en el sistema. Requiere planificación de diseño.
- **Soporte de Cifrado:** El nivel de protección cifrado que va a tener.
- **Gestión de Seguridad:** Gestión de perfiles de usuario y niveles de acceso vinculados al mismo.
- **Privacidad:** Soporte del anonimato de usuarios.
- **Capacidades de Autodefensa:** Controles para fallar de manera contenida o prevista. Ej: Reiteración de ingresos al sistema.
- **Control de Acceso:** información solo accesible a quien la necesita y este autorizado para ello. Manejo de la cantidad y tiempo de las sesiones, concurrencia e información.
- **Rutas o Canales Fiables:** Mecanismos que permitan confiar en los recursos accedidos.

Función de Hash

Se utilizan con relación a términos de seguridad. Cumplen una función no reversible, es decir, una vez “hasheado” el dato, no se puede volver a obtener su valor original.
Se representa en un valor fijo, donde si un elemento del archivo es modificado, el código hash cambia notablemente.
Existen diversos tipos, diferentes tipos de algoritmos implementan diferentes funciones de hash.
El hash se implementa sobre el archivo en sí y no sobre su fecha de modificación, de esta manera se sabe si el archivo sufrió una modificación.



Seguridad Lógica

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos. Esto se puede prever por medio de:

- **Controles de Acceso**
- **Identificación y Autenticación**
- **Roles**
- **Transacciones**
- **Limitaciones a los Servicios**
- **Modalidad de Acceso**
- **Ubicación y Horario**
- **Control de Acceso Interno**
  - Palabras Claves (Passwords)
  - Cifrado
  - Listas de Control de Accesos
  - Limites sobre la Interfaz de Usuario
  - Etiquetas de Seguridad
- **Control de Acceso Externo**
  - Dispositivos de Control de Puertos
  - Firewalls o Puertas de Seguridad
  - Acceso de Personal Contratado o Consultores
  - Accesos Públicos
- **Administración**

Referencia BYOD

Política empresarial que le permite a los empleados de una empresa traer sus propios dispositivos tecnológicos aceptando así el uso personal y empresarial de los mismos.

Rastreo y Gestión Remota de Dispositivos

Software que permite realizar operaciones de forma remota sobre el equipo permitiendo las siguientes acciones:

- Rastreo de dispositivo
- Borrado de datos
- Bloqueo de dispositivo
- Obtención de información

Rastreo y Gestión Remota

- **Prey (Multiplataforma)**
- **Cerberus**
- **Avast Anti-Theft**

- **Android**
- **Iphone**

Niveles de seguridad

El estándar más utilizado es el TCSEC. Los niveles describen diferentes tipos de seguridad del S.O. Estos niveles fueron la base de las ISO/IEC.

- **Nivel D - División Simple:** Contiene solo la división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad.
- **Nivel C1 – Protección Discrecional:** Requiere identificación de usuarios que permite el acceso a distinta información. Hace distinción de roles y cada uno maneja su propia información. Debe cumplir dos requerimientos:
  - Acceso de Control Discrecional: Distinción de usuarios y recursos.
  - Identificación y Autenticación.
- **Nivel C2 – Protección de Acceso Controlado:** Mayor cantidad de restricciones que C1. Capacidad de restringir que los usuarios ejecuten y/o tengan acceso a ciertas funciones del S.O. Requiere auditoria, la cual lleva registro de todas las actividades relacionadas con la seguridad.
- **Nivel B1 – Seguridad Etiquetada:** Soporta seguridad multinivel. El dueño del archivo no puede modificar los permisos de un objeto que esta bajo control de acceso obligatorio. A dicho objeto se le asigna una etiqueta y cada usuario deberá posee el permiso expreso para poder acceder al mismo y/o viceversa.
- **Nivel B2 – Protección Estructurada:** Existe una estructura de objeto en la cual el objeto de nivel superior debe estar etiquetado por ser el padre del objeto inferior. Si no se accede al padre, no se puede acceder al hijo.
  El sistema es capaz de alertar a los usuarios si sus condiciones de seguridad y accesibilidad son modificadas.
- **Nivel B3 – Dominios de Seguridad:** Refuerza los dominios con la instalación de hardware. Por medio de un monitor de referencia, se reciben las peticiones de acceso de cada usuario y las permite o deniega según las políticas de acceso definidas. Requiere que la terminal del usuario este conectada mediante una conexión segura.
- **Nivel A – Protección Verificada: :** Nivel de seguridad mas alto. Incluye un proceso de diseño, control y verificación, mediante métodos matemáticos para asegurar todos los procesos que realiza un usuario sobre el sistema. El software y hardware se encuentran protegidos para evitar infiltraciones ante traslados o movimientos de equipos.

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

- Firewalls
- Firewalls Personales
- Escaners de Vulnerabilidades
- Honeypots, Honeynets, Padded cells
- Verificadores de integridad
- IDS (Intrusion Detection System)
- IPS (Intruction Protection System)
- Antivirus
- WAF (Web Application Firewall)

Referencia VPN

Es una estructura de red que permite que por medio de una red pública y/o privada, se transmitan datos y/o información privada mediante el uso de criptografía.
Sus protocolos suelen ser IPSec, SSL/TLS, PPTP, L2TP

Seguridad Física

Mecanismos destinados a proteger físicamente cualquier recurso del sistema de amenazas producidas tanto por el hombre como por la naturaleza.

Calificación

- **Tipos de Desastres**
  - Desastres naturales, incendios accidentales, tormentas e inundaciones.
  - Disturbios, sabotajes internos y externos deliberados.
  - Amenazas ocasionadas por el hombre
- **Acciones Hostiles**
  - Robo
  - Fraude
  - Sabotaje
- **Control de Accesos**
  - Utilización de Guardias
  - Utilización de Detectores de Metales
  - Utilización de Sistemas Biométricos
  - Verificación Automática de Firmas (VAF)
  - Seguridad con Animales
  - Protección Electrónica

Prácticas de Seguridad Física en Móviles

- 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 de impactos.
- Utilizar contenedores de transporte que protejan al dispositivo del contacto con líquidos.