UNIVERSIDAD NACIONAL DE LA MATANZA

Departamento de Ingeniería e Investigaciones Tecnológicas

Seguridad y Calidad en Aplicaciones Web

Unidad N° 1: Introducción a la Seguridad

Referente de Cátedra: Walter R. Ureta
Plantel Docente: Cintia Gioia, Juan Monteagudo,
Walter R. Ureta

Información

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 **información** deriva del sustantivo latino *informatio(-nis)* del verbo *informare*, con el significado de "dar forma a la mente","disciplinar", "istruir", "enseñar".

Características de la información

Crítica:

Es indispensable para la operación de la organización

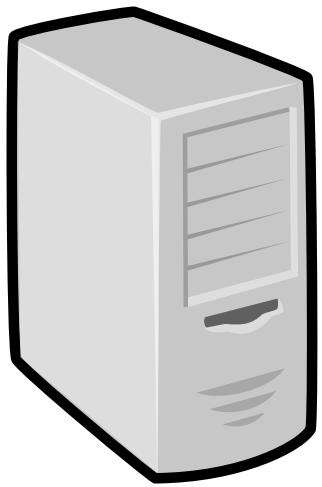
Valiosa:

Es un activo apreciado por la organización y sus operaciones.

Sensitiva:

Debe de ser conocida por las personas autorizadas

Contenedores de Información



Sistemas Aislados

Sistemas Interconectados

Seguridad

Proviene del latín *securitas*, que a su vez deriva de *securus* (sin cuidado, sin precaución, sin temor a preocuparse), que significa libre de cualquier peligro o daño.

Desde el punto de vista psicosocial se puede considerar 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.

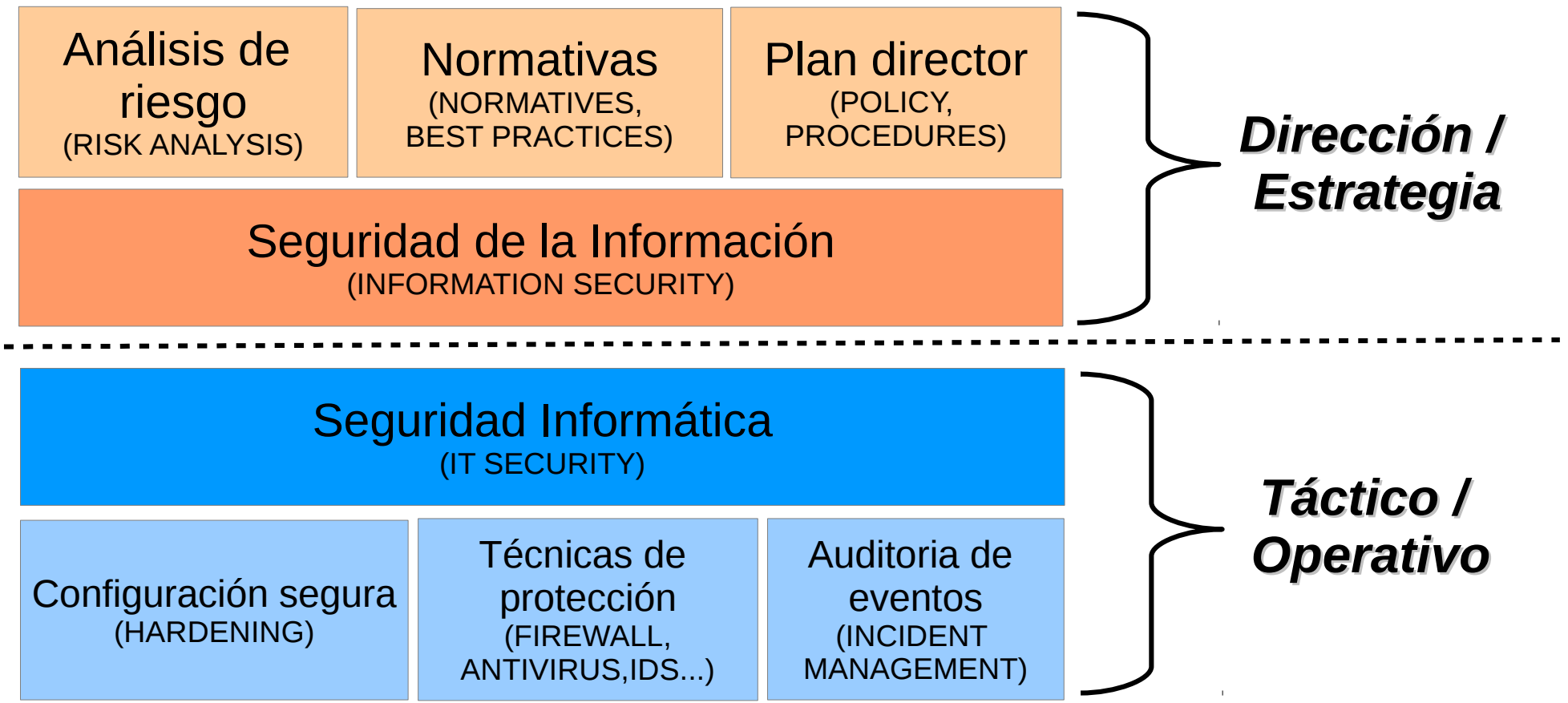
Seguridad de la Información

"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." *[Jeimy J. Cano, Ph.D., CFE.]*

Seguridad Informática

"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 de gobierno de tecnología de información* — 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." *[Jeimy J. Cano, Ph.D., CFE.]*

Seguridad Aplicada



Las causas de inseguridad

- Un **estado de inseguridad activo**; es decir, la falta de conocimiento del usuario acerca de las funciones del sistema puede hacerle tomar una acción que genere una exposición o vulnerabilidad *(por ejemplo, desactivar el antivirus del equipo)*

- Un **estado de inseguridad pasivo**; es decir, la falta de conocimiento de las medidas de seguridad disponibles *(por ejemplo, cuando el administrador o usuario de un sistema no conocen las funciones de seguridad con los que cuentan, como por ejemplo forzar la autenticación en el sistema)*

Términos relevantes

Riesgos

Amenazas

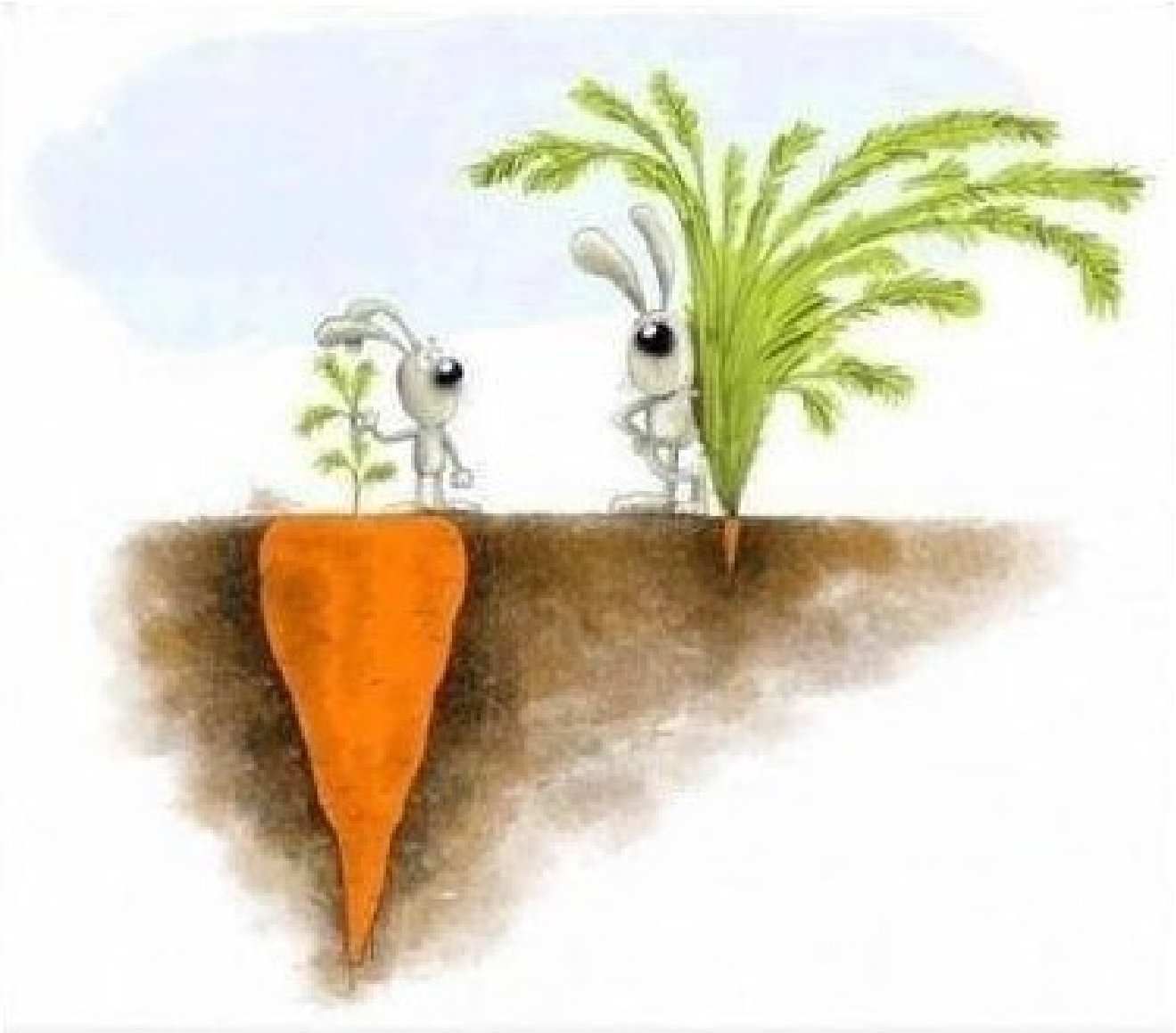
Vulnerabilidades

Términos relevantes

- Confidencialidad
- Integridad
- Disponibilidad
- No Repudio
- Anonimato
- Enfoque global

Triangulo ID

Requisitos funcionales para la seguridad



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 usuarios.
- **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 Lógica

Seguridad Lógica

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

Seguridad Lógica

- Controles de Acceso
- Identificación y Autentificación
- Roles
- Transacciones
- Limitaciones a los Servicios
- Modalidad de Acceso
- Ubicación y Horario
- Control de Acceso Interno
  - Palabras Claves (Passwords)
  - Encriptación
  - Listas de Control de Accesos
  - Límites sobre la Interfase de Usuario
  - Etiquetas de Seguridad

Seguridad Lógica

- Control de Acceso Externo
  - Dispositivos de Control de Puertos
  - Firewalls o Puertas de Seguridad
  - Acceso de Personal Contratado o Consultores
  - Accesos Públicos

- Administración
  - Administración del Personal y Usuarios - Organización del Personal

Practicas de Seguridad Lógica en móviles

- 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/o bloqueo remoto.
- Evitar o restringir conexiones a redes publicas 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 gestión remota de dispositivos

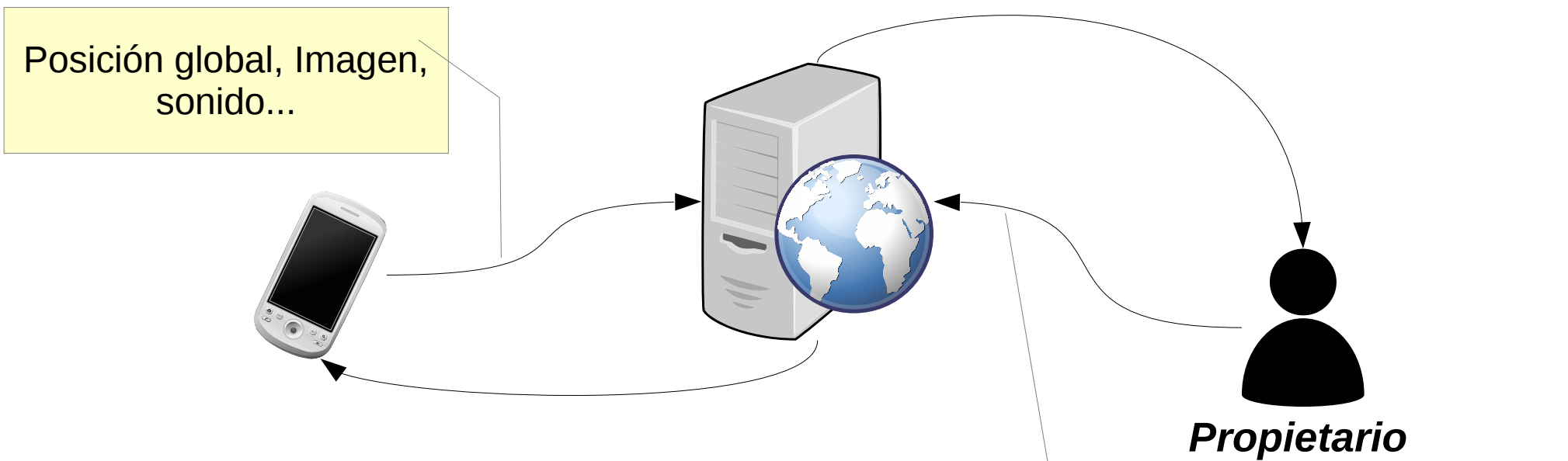
Este tipo de software permite realizar operaciones de forma remota sobre el equipo permitiendo el siguiente tipo de acciones:

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

Son aplicaciones particularmente útiles ante situaciones de **pérdida** y **robo**.

Su funcionalidad suele estar limitada por la conectividad del equipo.

Rastreo y gestión remota



- Prey *(Multiplataforma)*
- Cerberus
- Anti-robo & Find My Phone
- Avast Anti-Theft
- Android *(Ajustes/ Seguridad / Administradores del dispositivo)*

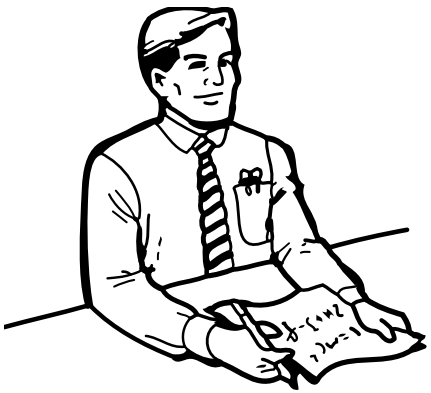
Seguridad Lógica

- Niveles de Seguridad
  - Nivel D, división simple
  - Nivel C1: Protección Discrecional
  - Nivel C2: Protección de Acceso Controlado
  - Nivel B1: Seguridad Etiquetada
  - Nivel B2: Protección Estructurada
  - Nivel B3: Dominios de Seguridad
  - Nivel A: Protección Verificada

Seguridad Lógica

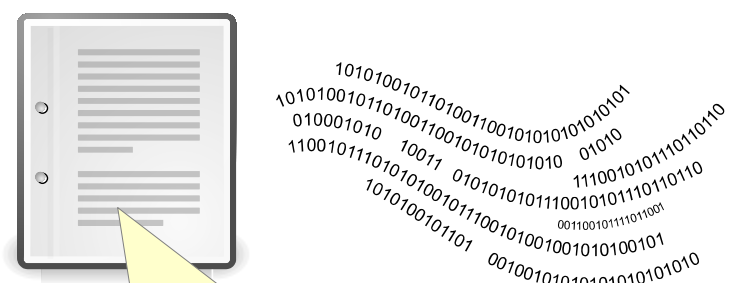
Estos son otros elementos comunes en el manejo de la seguridad lógica de sistemas:

- Firewalls
- Firewalls personales
- Escaners de vulnerabilidades
- Honeypots, Honeynets, Padded cells
- Verificadores de integridad
- IDS(*Intrusion Detection System*)
- IPS(*Intrusion Protection System*)
- Antivirus

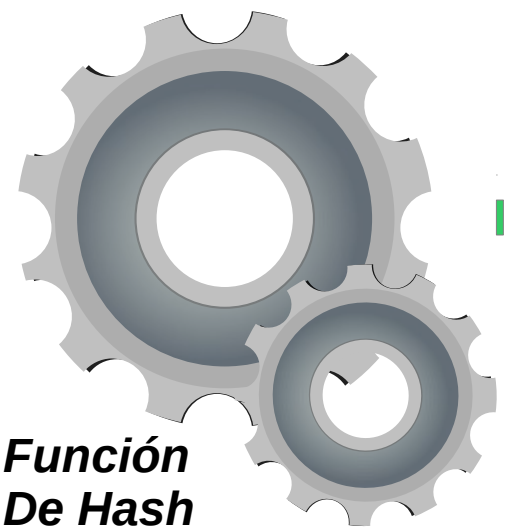


Referencia: Función de Hash

Se define como una función o método no reversible para generar un valor que represente de manera casi unívoca a un dato.



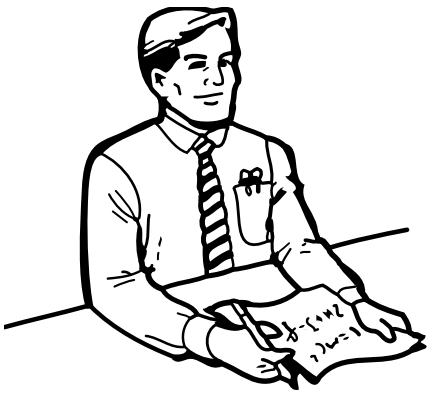
Información de entrada de tamaño variable



Función De Hash

0010101010101010

Información de salida de tamaño fijo y reducido



Referencia: VPN

Una estructura de red que con soporte lógico que permite el trafico de información privada sobre una infraestructura de red pública mediante el uso de criptografía.

Protocolos

- IPSec
- SSL / TLS
- PPTP, L2TP

Seguridad Física

Seguridad Física

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.

Seguridad Física

- 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

Practicas de Seguridad Física en móviles

- Evitar o restringir la manipulación del dispositivo en zonas publicas.
- 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 organización

Impacto en 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 través 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 de políticas
- 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

http://www.bligoo.com/media/users/1/50369/files/cisco_security_index_may08.pdf

Plan de concientización del personal

Periodo Difusión	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Posters		X		X		X		X		X		X
ScreenSavers			X		X		X		X		X	
Boletín		X			X		X		X		X	
Correo Electrónico			X			X		X		X		X
Capacitación trad		X	X	X								
Ferias de Tecnología				X								
Inducción	X	X	X	X	X	X	X	X	X	X	X	X
Alertas de Seguridad	X	X	X	X	X	X	X	X	X	X	X	X
Concurso de Seguridad				X								X
Videoconferencia		X	X	X								

Posters de concientización y otras ayudas:
http://stopthinkconnect.org/tips-and-advice/spanish-tips-and-advice/
http://nativeintelligence.com/posters/posters.asp

Plan de concientización del personal