AUDITORÍA DE LA SEGURIDAD FÍSICA, LÓGICA Y AMBIENTAL

Cátedra: Auditoría Informática

Seguridad FÍSICA

- Mecanismos de prevención y detección destinados a proteger **físicamente** cualquier recurso del sistema.
- Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y detección ante amenazas a los **recursos y a la información** confidencial".

¿Porque AUDITAR?

ISO (Organización Internacional de Normalización) 27001

"Seguridad de la información, ciberseguridad y protección de la privacidad"

La ISO 27001:2022 es la **norma internacional** para los sistemas de gestión de la seguridad de la información (SGSI). Proporciona un **marco** robusto para proteger la información y se puede adaptar a **organizaciones de todo tipo y tamaño**.

Las organizaciones más expuestas a los riesgos relacionados con la seguridad de la información eligen cada vez más implementar un **SGSI** que cumpla con la norma ISO 27001.

ISO (Organización Internacional de Normalización) 27002
CONTROLES

La mayoría de los negocios dispone o tiene acceso a **información sensible**. El hecho de no **proteger adecuadamente** dicha información puede tener **consecuencias** operativas, financieras y legales graves, que pueden incluso llevar a la quiebra del negocio.

El **reto** que la mayoría de negocios afronta es el de proporcionar una **adecuada protección**. Particularmente, cómo asegurar que han **identificado los RIESGOS** a los que están expuestos y **cómo gestionarlos** de forma proporcionada, sostenible y efectiva.

Tópicos de la Seguridad Física

1. **Áreas Seguras**

El objetivo es evitar el **acceso físico no autorizado**, los daños e interferencias a la **información** de la organización y a las **instalaciones de procesamiento** de la información.

2. **Seguridad de los equipos**

El objetivo es evitar la **pérdida, los daños, el robo** de activos comprometidos y que produzcan la interrupción de las operaciones de la organización.

Seguridad Física

- **Areas seguras y Seguridad de los equipos (14 Controles físicos)**

  - Perímetros de seguridad física
  - Entrada física
  - Seguridad de oficinas, salas e instalaciones
  - Monitoreo de seguridad física
  - Protección contra amenazas físicas y ambientales
  - Trabajar en áreas seguras
  - Escritorio claro y pantalla clara
  - Ubicación y protección de equipos
  - Seguridad de los activos fuera de las instalaciones
  - Medios de almacenamiento
  - Utilidades de soporte
  - Seguridad del cableado
  - Mantenimiento del equipo
  - Eliminación segura o reutilización del equipo

Áreas seguras y seguridad de los equipos

Una falta de control de los **accesos físicos** permite la materialización de potenciales amenazas, como:

- **Daños físicos** (agua, fuego, polución, accidentes, destrucción de equipos, polvo, corrosión, congelación, etc.)

- **Eventos naturales** (climáticos, sísmicos, volcánicos, meteorológicos, inundaciones, etc.)

- **Pérdida de servicios esenciales** (energía eléctrica, telecomunicaciones, aire acondicionado/agua, etc.)

- **Compromiso de información** (espionaje en proximidad, robo de equipos o documentos, divulgación, recuperación desde medios deshechados, manipulación de hardware, manipulación de software, etc.)

Áreas seguras y seguridad de los equipos

1. Perímetros de seguridad física

Se deberán *definir y utilizar* perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.

los lugares (instalaciones y entorno), los edificios, las áreas públicas y dentro de la empresa, las áreas de trabajo y las áreas seguras a proteger.

Áreas seguras y seguridad de los equipos

1. Perímetro de seguridad física

Tener en cuenta los siguientes elementos de protección:

- 1.- El emplazamiento de la empresa (vallas o muros) o el edificio (paredes y ventanas).
- 2.- La antigüedad del edificio y la calidad de su estructura.
- 3.- Los sectores o divisiones dentro del edificio.
- 4.- Los armarios, cajas fuertes o elementos más pequeños donde se guardan los activos de información.

Áreas seguras y seguridad de los equipos

2. Entrada física

Las áreas seguras deberán estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.

Áreas seguras y seguridad de los equipos

2. Entrada física

IDENTIFICACION DE ACTIVOS

- Elaborar un **inventario** de activos informáticos.
- Definir propietarios (**responsables**) de activos informáticos.
- Especificar a los propietarios de activos informáticos las autorizaciones de acceso (**tipo de acceso y validez**).

Áreas seguras y seguridad de los equipos
2. Entrada física

ACCESO A LAS AREAS CRITICAS

- Disponer de un **control de acceso** físico al centro de datos.
- Elaborar un **procedimiento de control** de acceso físico.
- Disponer de **un registro de los accesos físicos** (identificando día, hora, ingresantes y motivo).
- **Asegurar el sistema de registro** del control de acceso.

Áreas seguras y seguridad de los equipos
2. Entrada física

Proteger recursos e información

- ✓ Saber quién accede.
- ✓ Saber cuándo accede.
- ✓ Saber a qué accede.
- ✓ Evita que lo haga quien no debe o cuándo no debe.

Áreas seguras y seguridad de los equipos
2. Entrada física

- ✓ No acceder a más ni menos de lo que se necesita.
- ✓ No disponer de acceso durante más tiempo del necesario.
- ✓ No acceder con más permisos de los necesarios.
- ✓ No conceder permisos a más usuarios de los indispensables.
- ✓ Disponer de varios perfiles para funciones diferenciadas.

Áreas seguras y seguridad de los equipos
3. Seguridad de oficinas, habitaciones e instalaciones

Control Preventivo

Se deberá diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.

CPD – Requisitos áreas críticas

- Disponibilidad 24*7*365.
- Fiabilidad infalible 99,99% de disponibilidad. No más de 1 hora de fallos al año.
- Seguridad, redundancia y diversificación. Almacenaje de datos, tomas de alimentación eléctrica independientes, control de acceso, etc.
- Control ambiental y prevención de incendios.
- Acceso a Internet y conectividad a redes área extensa.

CPD - Climatización

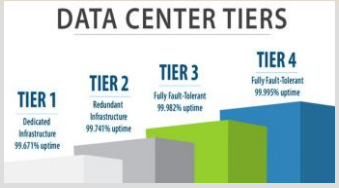
- Aires acondicionados.
- Eliminar calor e inyectar aire en la sala (pasillos fríos).
- Condiciones óptimas de temperatura (17°-19°).
- Humedad: 45%.
- Servidores con disipadores y turbinas en lugar de ventiladores.

CPD – Sistemas de Seguridad

✓ Sistemas Contra incendios
Material ignífugo.
Detectores, extintores, mangueras, etc.

✓ Sistemas Eléctricos
Estimar carga a soportar.
Canalizaciones para aislar los cables
Aislamiento contra interferencias, humedades, etc.
Separar líneas eléctricas de las de datos.
Sistema de Alimentación Ininterrumpida (SAI).

Estándar de Uptime Institute TIA-942



Se diferencian en aspectos como el tiempo que los sistemas permanecen conectados y sin caídas, la seguridad de los centros ante ciberataques y desastres naturales, así como las características de las infraestructuras, o los materiales utilizados y la redundancia de los sistemas. Esto último se refiere a contar con componentes por duplicado, por si uno de ellos falla, existe otro igual de *back up*.

Nuevo Data Center de Claro

EMPRESAS

Claro invierte US$ 30 millones en un nuevo data center en Buenos Aires

La empresa propiedad del mexicano Carlos Slim abrirá nuevas oficinas con un diseño sustentable en el barrio de San Telmo

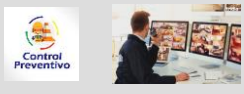
SERGIO LANZAFAME
viernes, 30 de agosto de 2024 · 23:50 hs

Nuevo Data Center de Claro

- Según remarcó la empresa en un comunicado, el nuevo edificio se destacará por su diseño modular, un enfoque que permite la construcción en etapas y que fue seleccionado por sus beneficios en términos de escalabilidad y sostenibilidad. **Al optar por una construcción modular, Claro Argentina podrá adaptar y expandir el centro de datos según las necesidades futuras, mientras que se minimizan los costos y tiempos de construcción.**
- El data center está siendo construido bajo el **estándar Tier III del Uptime Institute**, una certificación internacional que **garantiza un alto nivel de disponibilidad y redundancia en las operaciones**. Esto significa que el centro de datos **estará preparado para funcionar sin interrupciones, incluso en situaciones adversas, lo que es crucial para garantizar la continuidad de servicios críticos. La certificación Tier III también implica que el edificio contará con sistemas avanzados de gestión de energía para reducir el consumo y minimizar la huella de carbono**.

Áreas seguras y seguridad de los equipos

4. Monitoreo de seguridad física



Las instalaciones deben ser monitoreadas continuamente para detectar y disuadir el acceso físico no autorizado.

Áreas seguras y seguridad de los equipos

5. Protección contra amenazas físicas y ambientales

Se deberá diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.

Eventos naturales:

climáticos, sísmicos, volcánicos, meteorológicos, inundaciones, etc.

PLAN DE CONTINGENCIA

Disponer de un Plan de Contingencia adecuado ante un DESASTRE

Desastre: Es cualquier evento , que cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa

Probabilidad BAJA, pero si ocurre puede ser FATAL

Los medios necesarios para afrontar el Desastre quedan definidos en el Plan de Recuperación de desastres, que junto con el Centro Alternativo de Proceso de Datos constituyen el PLAN DE CONTINGENCIA

PLAN DE CONTINGENCIA

- Establecer Quiénes, y Cómo deben elaborar el plan, implementarlo, probarlo y mantenerlo; qué contemplar y dónde se debe desarrollar el plan.
- **MARCO DEL PLAN**:

¿Debe limitarse a los equipos centrales?
¿Debe incluir los equipos departamentales, PC's y LAN's?
¿Qué procesos son, estratégicamente, más importantes?

PLAN DE CONTINGENCIA

- **ORGANIZACION**:

¿Quiénes deben componer el equipo de desarrollo del plan?

¿Quién será el responsable de este equipo?

¿Cómo se relacionarán con el resto de la institución?

¿Qué nivel de autonomía tendrá el equipo?

¿A quién reportará?

- **Apoyo institucional. Comunicación e importancia estratégica.**

CPD - Centros de Respaldo

- **Sala Fría**
  CPD con toda la infraestructura necesaria.
- **Sala Caliente**
  CPD con restauración solo de los datos.
- **Mutual Backup**
  Acuerdo entre organizaciones para backups mutuos.
- **Centro espejo**
  Replicación en tiempo real.

Áreas seguras y seguridad de los equipos
6. Trabajar en áreas seguras

Se deberán diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.

Control Preventivo

Áreas seguras y seguridad de los equipos
6. Trabajar en áreas seguras

Se deberán controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.

Áreas seguras y seguridad de los equipos
7. Escritorio claro y pantallas claras

Se debería adoptar una política de puesto de trabajo despejado para ***documentación en papel y para medios de almacenamiento*** extraíbles y una política de ***monitores sin información*** para las instalaciones de procesamiento de información.

Control Preventivo

MEDIDAS a Implementar

Buenas Prácticas

- Escritorios Limpios para Proteger Documentos en Papel y Dispositivos de Almacenamiento Removibles
- Políticas de Pantallas Limpias
- Documentos Importantes en Papel y Medios de Información, deben almacenarse Bajo Llave
- Información Sensible debe guardarse en Caja Fuerte o Bóveda a Prueba de Incendio

MEDIDAS a Implementar

Buenas Prácticas

- Las PCs, Terminales e Impresoras NO deben dejarse conectadas cuando están desantendidas
- Proteger Puntos de Recepción y Envío de Correo, Fax y Telex
- Las Fotocopiadoras deben estar bloqueadas fuera del Horario Normal de Trabajo

- La Información Sensible Impresa debe retirarse inmediatamente de la Impresora
- No se debe retirar nada de la Organización sin debida Autorización

Áreas seguras y seguridad de los equipos

8. Ubicación y protección de equipos

Control Preventivo

Los equipos se deberán ubicar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.

Áreas seguras y seguridad de los equipos

9. Seguridad de los activos fuera de las organizaciones

Control Preventivo

Los equipos, la información o el software no se deberán retirar de la organización sin previa autorización.

Áreas seguras y seguridad de los equipos

9. Seguridad de los activos fuera de las organizaciones

Control Preventivo

Se deberá aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.

Áreas seguras y seguridad de los equipos

10. Medios de almacenamiento

Control Preventivo

Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización para garantizar solo la divulgación, modificación, eliminación o destrucción autorizada de la información almacenada

Áreas seguras y seguridad de los equipos

10. Medios de almacenamiento

- Retiro de la organización
- Almacenamiento en lugar seguro
- Uso de técnicas criptográficas para protección
- Mitigar riesgos de degradación
- Múltiples copias y lugares separados

Áreas seguras y seguridad de los equipos

11. Utilidades de soporte

Control Preventivo

Las instalaciones de procesamiento de información deben estar protegidas contra cortes de luz y otras interrupciones provocadas por fallas en los servicios públicos de apoyo, para evitar la pérdida, el daño o el compromiso de la información o la interrupción de las operaciones de la organización.

Áreas seguras y seguridad de los equipos

12. Seguridad del cableado

Control Preventivo

Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberán proteger contra la intercepción, interferencia o posibles daños.

Áreas seguras y seguridad de los equipos
13. Mantenimiento de los equipos

Control Preventivo

Los equipos deberán mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

Áreas seguras y seguridad de los equipos
14. Eliminación segura o reutilización del equipo

Control Preventivo

Se deberán verificar todos los equipos que contengan medios de almacenamiento, para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

FUENTES de la Auditoría Física

Un Centro de Cómputos sigue un modelo organizativo más o menos estándar, según:

- Tipo de Empresa,
- Situación Económica,
- Disponibilidad de Espacio,
- Actitud de la Dirección, etc.

Permiten distinguir que los Centros de Cómputos difieren bastante unos de los otros

FUENTES de la Auditoría Física

Deberían estar accesibles en todo Centro de Cómputos:

- Políticas , Normas y Planes de Seguridad emitidos y distribuidos
- Auditorías anteriores, generales o parciales referidas a Seguridad Física o relacionado a ella
- Contratos de Seguros, de Proveedores y de Mantenimiento
- Actas e Informes de Técnicos y Consultores sobre el Edificio, Electricidad, Aire, etc.
- Informes de Accesos y Visitas
- Informes sobre Pruebas de Evacuación
- Políticas del Personal. Proceso de cancelación de Contratos y Despidos, Rotación en el Trabajo, Contratos Fijos y Temporales
- Inventarios de Soportes (Cintoteca, Back-up, Procedimientos de Archivos, Controles de Salida y Recuperación de Soporte, Control de Copias, etc.)
- Entrevistas con Personal deseado

TÉCNICAS y herramientas del Auditor

- Entrevistas con **Directivos y Personal Fijo o Temporal** (no es interrogatorio)
- Consultas a **Técnicos y Peritos** que formen parte de la plantilla o independientes

TÉCNICAS y herramientas del Auditor

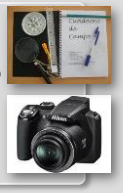
- **Revisión analítica de:**
  - Documentación sobre Construcción y Pre-instalaciones
  - Documentación sobre Seguridad Física
  - Políticas y Normas de Actividad de Sala
  - Normas y Procedimientos sobre Seguridad Física de los Datos
  - Contratos de Seguros y de Mantenimiento

TÉCNICAS y herramientas del Auditor

- Observación de las **Instalaciones, Sistemas, Cumplimiento de Normas y Procedimientos**, etc. (Tanto de **Espectador** como **Actor**)

TÉCNICAS y herramientas del Auditor

- **Herramientas:**
  - Cuaderno de Campo / Grabadora de Audio
  - Máquina Fotográfica / Cámara de Video
    - Su uso debe ser discreto y con la debida autorización.



PREGUNTAS?