Sistemas de Gestión de Seguridad de la Información

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Sistemas de Gestión de Seguridad de la Información

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Google Data Center security

¿Qué es la seguridad física?

Mecanismos de detección y prevención

Orientados a proteger físicamente los recursos del sistema

Aplicación de barreras físicas y procedimientos de control contra las amenazas a los recursos

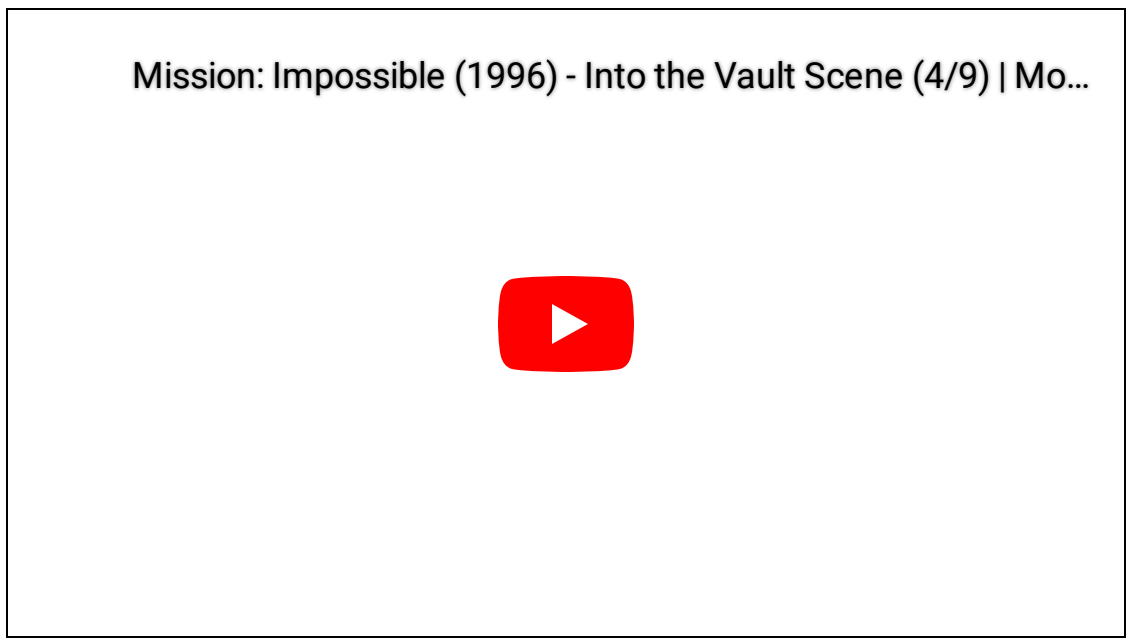
¿De qué sirve tener el software protegido contra hackers si cualquiera puede llevarse el ordenador?

¿Qué es la seguridad física?

Cámara acorazada en la CIA: Acceso por escáner de retina, Acceso con huella dactilar, Acceso con sensor de voz, Sensor de movimiento, Sensor de sonido, Sensor de temperatura, Sensor de presión en el suelo

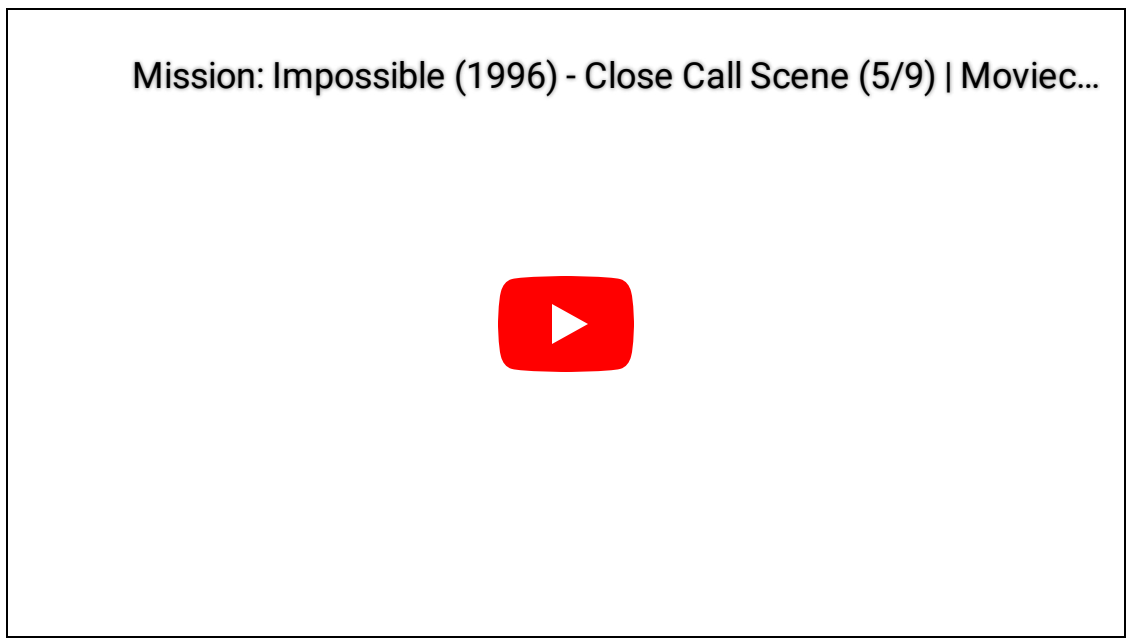
¿Qué es la seguridad física?

Sensor de temperatura



¿Qué es la seguridad física?

Sensor de presión en el suelo



¿Qué es la seguridad física?

El PC tiene un simple password!

¿Qué es la seguridad física?

La seguridad física es tan importante como la lógica:

- Debe ser coherente con el valor de la información a proteger
- Las medidas de seguridad deben ser equilibradas
- Las medidas de seguridad deben aplicarse también a los servicios que ofrece la empresa

Estándares y normas de seguridad

ISO (International Organization for Standardization, 1947): organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización

AENOR (Asociación Española de Normalización y Certificación, 1986): desarrolla actividades de normalización y certificación (N+C), para mejorar los productos y servicios

Estándares y normas de seguridad

ISO 27002

Define las medidas para gestionar la seguridad de los sistemas de información

Capítulo 9 - Control de accesos: Define todo lo relativo a controlar los accesos de los usuarios a los recursos / servicios de la empresa

Estándares y normas de seguridad

ISO 27003

Describe los pasos a seguir para diseñar un SGSI

Como resultado de su aplicación se obtiene un plan de implementación del SGSI

Estándares y normas de seguridad

ISO 27004: Define cómo medir la efectividad de un SGSI que ya esté implementado

ISO 27005: Define cómo elaborar un plan de riesgos

SGSI

Proceso PDCA (Plan-Do-Check-Act):

1. Planificar
2. Hacer
3. Comprobar
4. Actuar

Planificar (1)

Análisis pormenorizado de las áreas que componen nuestra organización que nos servirá para establecer una política de recuperación ante un desastre

Analisis de riesgos: plan de contingencia

- Se identifican las amenazas
- Se valoran las pérdidas si las amenazas se cumplen
- Se estima el coste de proteger la información

Planificar (1)

Plan de contingencia incorpora medidas:

- Técnicas
- Organizativas
- Humanas

Medidas Técnicas

Extintores contra incendios

Detectores de humo

Salidas de emergencia

Equipos informáticos de respaldo

Medidas Organizativas

Seguro de incendios

Precontrato de alquiler de equipos informáticos y ubicación alternativa

Procedimiento de backups

Procedimiento de actuación en caso de incendio

Medidas Humanas

Formación para actuar en caso de incendio

Designación de un responsable de sala

Asignación de roles y responsabilidades para la copia de seguridad

...

Planificar (1)

Plan de contingencia contiene subplanes:

- Respaldo
- Emergencia
- Recuperación

Planificar (1)

Plan de **Respaldo**:

- Qué hacer antes de que se produzca la amenaza
- Finalidad: prevenir la materialización de la amenaza
- Revisión de extintores, Simulacros de incendio, Realización de copias de seguridad (+ tests de recuperación), …

Planificar (1)

Plan de **Emergencia**:

- Qué hacer mientras se produce la amenaza o justo después
- Finalidad: paliar los efectos adversos de la materialización de la amenaza
- Activación del precontrato de alquiler de equipos informáticos, Restauración de las copias de seguridad, ...

Planificar (1)

Plan de **Recuperación**:

- Qué hacer una vez controlada la amenaza
- Finalidad: restaurar las cosas al estado en el que se encontraban antes de la materialización de la amenaza
- Evaluación de daños, Traslado de datos desde la ubicación de emergencia a la habitual, Desactivación del precontrato de alquiler, Reclamaciones a la compañía de seguros, …

Planificar (1)

El plan de **contingencia** no debe limitarse a enumerar una serie de medidas.

También debe incluir:

- Qué recursos materiales son necesarios
- Qué personas están implicadas en el cumplimiento del plan
- Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan
- Qué protocolos de actuación deben seguir y cómo son

Hacer (2)

Se implementan las contramedidas que se hayan estimado oportunas para proteger los bienes

Contramedidas de varios tipos: Atenuar los riesgos, Minimizar las pérdidas, Asegurar una rápida recuperación

Fundamental: formación e información al personal afectado

Comprobar (3)

Revisiones periódicas (auditorías)

Especialmente tras la materialización de una amenaza

Asegura:

- La puesta al día frente a nuevas amenazas
- El correcto funcionamiento del SGSI

Actuar (4)

Resultado de la comprobación

Amenaza prevista, contramedidas eficaces: revisar aspectos menores para mejorar la eficiencia

Amenaza prevista, contramedidas ineficaces: analizar causa de fallo y proponer nuevas contramedidas

Amenazas

Ocasionadas por los humanos

Ocasionadas por desastres naturales

Alteraciones del entorno

Acceso a información en soporte físico

Amenazas (Humanos)

¿Podría un ciberatacante acceder a sistemas informáticos cerrados y sin tocar directamente los equipos?

Amenazas (Humanos)

Amenazas (Humanos)

La posibilidad de acceder físicamente a un sistema puede hacer que las medidas de seguridad empleadas sean inútiles

Hay que establecer “áreas seguras”

A veces no hay ni que acceder físicamente al sistema (Ataque TEMPEST)

Amenazas (Humanos)

Las emanaciones electromagnéticas podrían ser un vector de ataque

¿Cómo captar las emanaciones electromagnéticas? Todos los aparatos electrónicos emiten radiaciones y emanaciones en forma de señales electromagnéticas y acústicas.

Amenazas (Humanos)

Dependiendo de diversos factores como la distancia y los obstáculos, se pueden captar las señales de los componentes a través de antenas o micrófonos de alta sensibilidad (en el caso de señales acústicas) y procesarlas para obtener información

Entre estos aparatos también se encuentran los **monitores** y **teclados**, por lo que estas técnicas pueden ser también empleadas por ciberatacantes

Amenazas (Humanos)

Las instalaciones de procesamiento de información crítica o sensible deben estar en áreas protegidas con un perímetro de seguridad definido por:

- Vallas
- Controles de acceso apropiados

La protección debe ser proporcional a los riesgos identificados

Amenazas (Humanos)

Control de acceso a un área protegida: Personal de seguridad, Llaves, Tarjetas de acceso, PIN , Sistema biométrico, ...

Amenazas (Humanos)

Sistemas biométricos: sistemas que identifican a las personas en base a una característica “física”:

- Huella digital
- Palma de la mano
- Patrones oculares
- Reconocimiento facial
- Verificación de voz
- Pautas al caminar

Amenazas (Humanos)

Los visitantes de áreas protegidas deben ser supervisados o inspeccionados

La fecha y hora de sus entradas y salidas debe quedar registrada

El acceso debe permitirse con propósitos específicos y autorizados

El visitante debe ser instruido en las medidas de seguridad del área

Amenazas (Humanos)

Los accesos deben ser auditados de manera periódica

La información de los accesos también debe ser protegida

Es recomendable llevar una identificación visible de manera continua

Alentar a los empleados a sospechar de personas no identificadas

Amenazas (Humanos)

No todos los empleados tienen porqué saber qué se hace en el área protegida

Las áreas protegidas desocupadas deben quedar bloqueadas

No se debe permitir el acceso a cámaras fotográficas, móviles, etc.

Amenazas (Humanos)

Inicio / **Política**

Fotos del príncipe Guillermo como piloto revelan información clasificada

EFE - Londres

20/11/2012 - 20:13h

Me gusta 0 Twittear 1

La web de los duques de Cambridge de Inglaterra tuvo que retirar hoy unas fotos del príncipe Guillermo como piloto militar después de que el Ministerio de Defensa británico advirtiera de que mostraban información clasificada.

Las imágenes se publicaron esta mañana en la web del príncipe Guillermo y la princesa Catalina, en un intento de mostrar el trabajo del nieto de Isabel II como capitán de la Real Fuerza Aérea Británica en la base de rescate de Anglesey (Gales).

Amenazas (Desastres naturales)

Terremotos, Fuego, Tormentas eléctricas, Inundaciones

Hay que contemplarlos en la política de seguridad de la empresa

Amenazas (Desastres naturales)

Pérdida de información

Pérdida de equipamiento

Tiempo en recuperarse = dinero

Resiliencia: capacidad de sobreponerse a una situación adversa

Amenazas (Desastres naturales)

¿Qué fue de las empresas que tenían su sede en la Torre Windsor (2005)?

En este edificio de oficinas se ubicaban principalmente empresas como la Consultora Deloitte (ocupando 20 de sus 32 plantas) o el Despacho de Abogados Garrigues

Amenazas (Desastres naturales)

Consultora Deloitte:

- Bien preparada
- El lunes siguiente trabajando en condiciones “normales”

Despacho de abogados Garrigues

- Copias de seguridad en otra planta del mismo edificio
- Perdieron grandes cantidades de información

Amenazas (Desastres naturales)

Consultora Deloitte:

Copias de seguridad externas de todos sus datos, y toda la información en documento físico tenía su copia en soporte informático.

Amenazas (Desastres naturales)

Consultora Deloitte:

Estos backups se gestionan en localizaciones distintas a las de la propia empresa, cumpliendo así con las normativas de seguridad, con la Ley de Protección de Datos (LOPD) y con la autoprotección de las propias empresas

Amenazas (Desastres naturales)

Según el Disaster Recovery Institute International, el 90% de empresas que experimentan pérdidas significativas de datos, quiebran en un plazo de 3 años

Las medidas de contingencia ante desastres, la salvaguarda de datos, es una tarea imprescindible para que una empresa tenga continuidad en el desarrollo de su negocio

Amenazas (Desastres naturales)

Según un estudio de la Universidad de Texas, sólo el 6% de empresas con pérdida catastrófica de datos sobrevivirá, frente a un 43% que nunca reabrirá su negocio y un 51% que tendrá que cerrar en un plazo de 2 años

Amenazas (Desastres naturales)

Periodo máximo de inactividad que puede soportar una empresa sin poner en peligro su supervivencia es de:

- Sector seguros: 5,6 días
- Sector fabricación: 4,9 días
- Sector industrial: 4,8 días
- Sector distribución: 3,3 días
- Sector financiero: 2,0 días

Amenazas (Desastres naturales)

Terremotos:

- Probabilidad según la localización
- Pequeñas vibraciones pueden estropear maquinaria delicada
- Obras en el entorno pueden producir vibraciones
- Soluciones preventivas
- Soluciones arquitectónicas
- Emplazamientos adecuados
- Protecciones del edificio

Amenazas (Desastres naturales)

Fuego:

- Una mala instalación eléctrica
- Descuidos personales como puede ser fumar en sala de ordenadores
- Papeleras mal ubicadas en la que se tira un cigarrillo no apagado
- Vulnerabilidades del sistema ante el humo

Amenazas (Desastres naturales)

Fuego (Soluciones preventivas):

- Detector humo y calor
- Materiales ignífugos
- Almacén de papel separado de máquinas
- Revisar el estado del falso suelo
- Extintores revisados

Amenazas (Desastres naturales)

Tormentas eléctricas:

- Subidas de tensión que afectan a los equipos
- Soluciones preventivas
- Limitadores de tensión
- Estabilizadores de corriente
- SAI (Sistema de Alimentación Ininterrumpida)

Amenazas (Desastres naturales)

Inundaciones y similares:

- Inundaciones por causas propias de la empresa
- Inundaciones por causas ajenas
- Pequeños incidentes personales (botella de agua, taza con café)

Amenazas (Desastres naturales)

Inundaciones y similares (Soluciones preventivas):

- Instalar sistemas de drenaje de emergencia
- Concienciación de los empleados
- Revisar conductos del agua
- Localización del equipamiento
    - A nivel general (NO en un sótano al lado de un rio)
    - A nivel del edificio (NO en una sala con grifos)

Amenazas (Desastres naturales)

Amenazas (Alteraciones del entorno)

- Temperaturas
- Polvo
- Insectos
- Soluciones preventivas
  - Sistemas de refrigeración
  - Limpieza
  - Cámaras acorazadas
  - Filtros en los conductos

Amenazas - Acceso a información en soporte físico

Cualquier dispositivo por el que se extraiga información confidencial debe encontrarse en un área de seguridad

- Nuevos dispositivos
- Permisos de impresión o extracción de datos sólo a los usuarios que realmente lo necesitan
- Imprimir sólo en presencia del usuario (tarjetas inteligentes)
- Revisión de los empleados al abandonar el área de seguridad