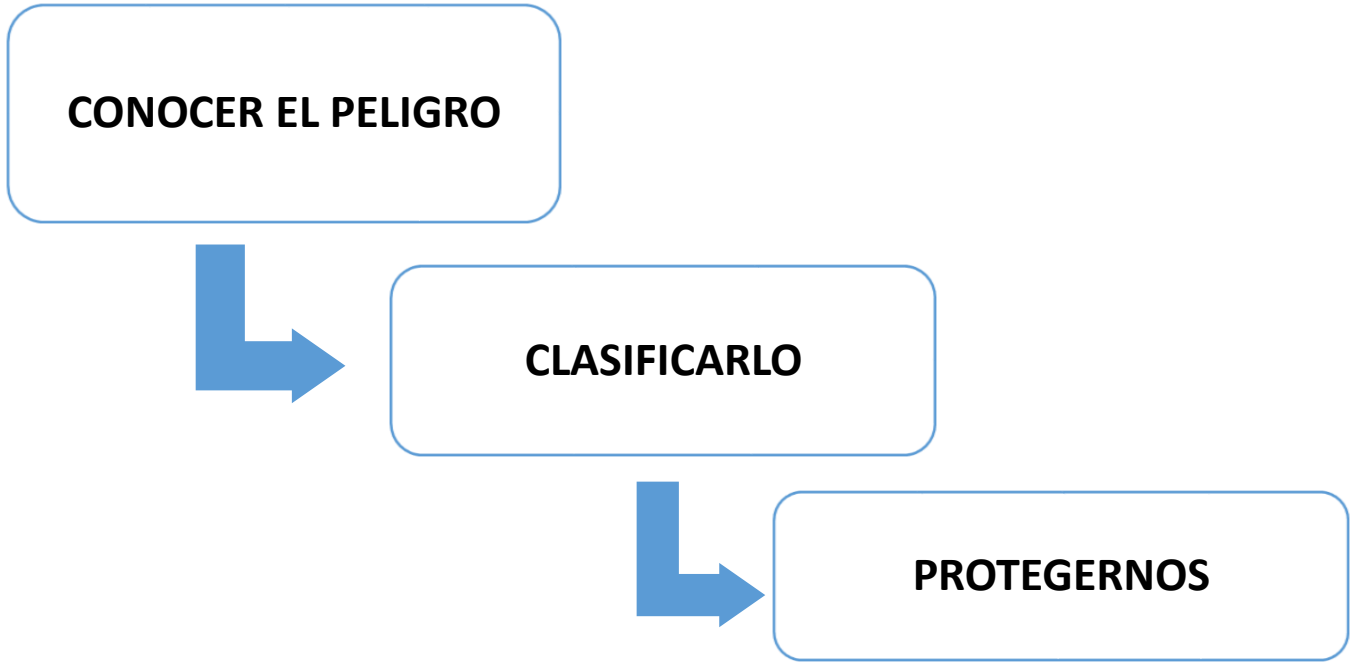
CRITERIOS SEGURIDAD EQUIPOS INFORMATICOS

SEGURIDAD INFORMÁTICA

- *Protección provista a un sistema de información para alcanzar los objetivos de preservar la **integridad**, **disponibilidad** y **confidencialidad** de los recursos del sistema de información, incluyendo software, hardware, firmware, datos/información y telecomunicaciones*

ES IMPORTANTE …



NORMATIVAS SEGURIDAD

norma ISO 17799 e ISO 27001

- Para la norma **ISO 17799** e **ISO 27001,** referencias obligadas en la seguridad de la información es

- **“la preservación de confidencialidad, integridad y disponibilidad de la información”.**

Ministerio de Administraciones Públicas : MAGERIT

- **Ministerio de Administraciones Públicas,** en su versión de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), define seguridad como
- **“la capacidad de las redes o de los sistemas de información, de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles**

SEGURIDAD INFORMATICA

SEGURIDAD INFORMÁTICA

Principios básicos de la seguridad

Confidencialidad los activos sólo han de poder ser accedidos por los elementos autorizados a ello

→ los elementos autorizados no van a poder hacer disponibles dichos activos a terceros no autorizados

Integridad los activos sólo pueden ser modificados (creación,modificación, eliminación) por elementos autorizados de modo que se salvaguarde su exactitud y completitud

Disponibilidad los activos tienen que permanecer accesibles y utilizables por parte de los elementos autorizados cuando estos los requieran

Fuga de información

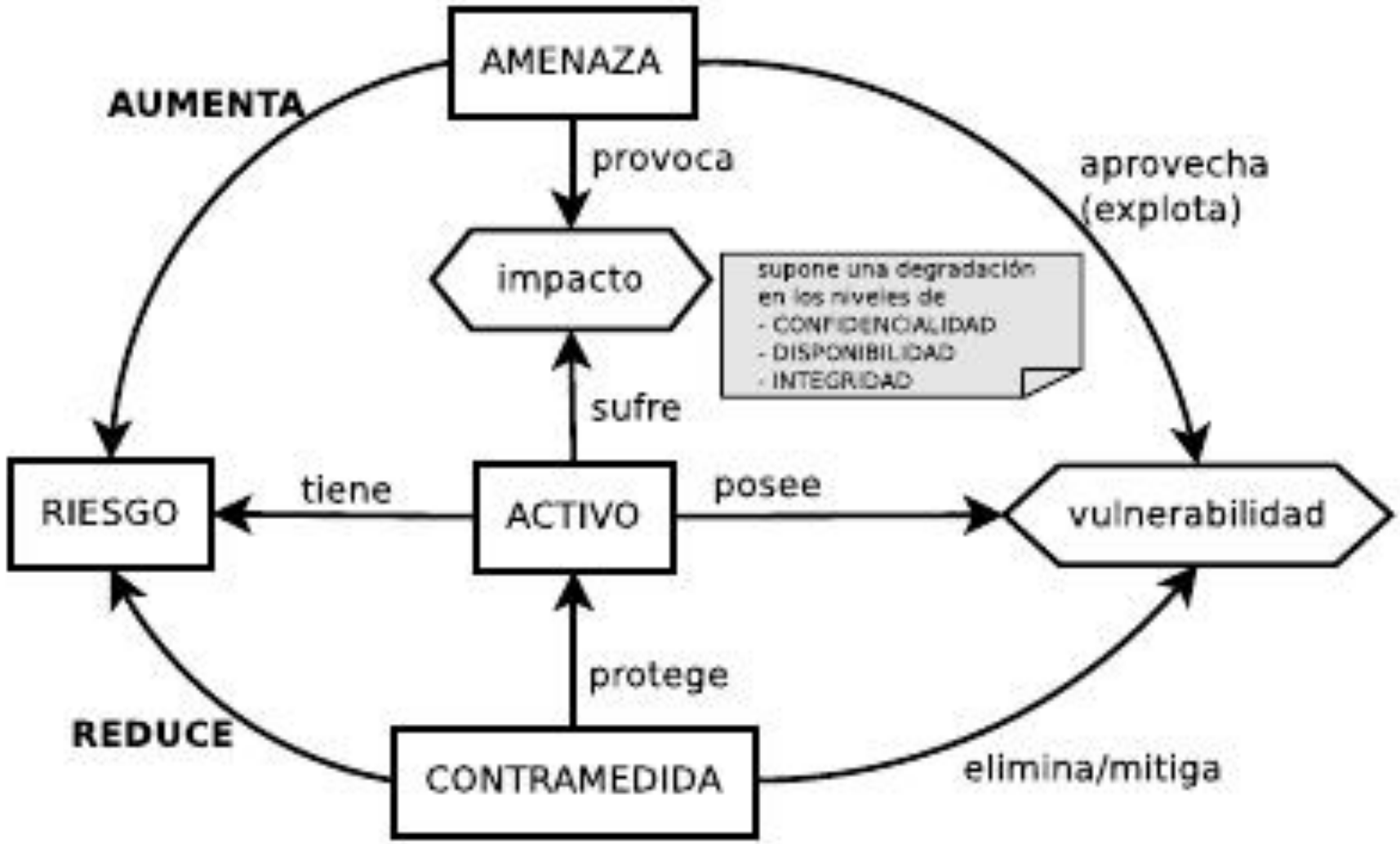
RESPETAR TRES PRINCIPIOS BÁSICOS

Confidencialidad	Información accesible sólo por el personal autorizado
Integridad de la información	Información correcta y libre de modificaciones y errores
Disponibilidad de la información	Información accesible cuando sea necesario

Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Mecanismos

- Los mecanismos de seguridad se implementan para proteger uno o más de estos principios
- Riesgo, amenazas y vulnerabilidades se miden en función de su capacidad de comprometer alguno de estos principios
- Son principios complementarios y contrapuestos deben balancearse


AMENAZA
AUMENTA
provoca
aprovecha
(explota)
impacto
supone una degradación
en los niveles de
- CONFIDENCIALIDAD
- DISPONIBILIDAD
- INTEGRIDAD
sufre
RIESGO
tiene
ACTIVO
posee
vulnerabilidad
protege
REDUCE
CONTRAMEDIDA
elimina/mitiga

ACTIVOS A PROTEGER

Activos

Cualquier recurso (tangible o intangible) con valor para una organización

Tipos de activos (según Libro II de la metodología MAGERIT ver. 3)

activos esenciales	información (datos personales, datos clasificados, ...), servicios
arquitectura del sistema	puntos de acceso al servicio, puntos de interconexión, ...
datos/información	ficheros, copias de seguridad, datos de configuración, credenciales, registros de control de acceso, registros de actividad, código fuente, ejecutables, datos de prueba, ...
claves criptográficas	claves de cifrado, claves de firma, certificados, soportes físicos cifrados, ...
servicios	internos, al público en general, a usuarios externos, web, correo electrónico, acceso remoto, directorio, tranferencia de ficheros, almacenamiento, ...
software/aplicaciones	desarrollo propio, desarrollo a medida, software estándar (navegadores, servidor de aplicaciones, ofimática, sistema operativo, antivirus, sistema de backup, ...)
equipamiento informático	grandes equipos, informática personal, informática móvil, equipo virtual, periféricos (impresoras, escaner, ...), dispositivos de red (modem, router, firewall, pasarela, punto de acceso inalámbrico....), centralita telefónica, ...
redes de comunicaciones	red telefónica, enlace punto a punto, ADSL, red inalámbrica, red local, telefónía móvil, ...
soportes de información	electrónicos (discos, cintas, CD/DVD, almacenamiento en red, memorias USB, ...) y y no electrónicos (papel impreso, microfilm, ...)
equipamiento auxiliar	cableado, SAI, climatización, mobiliario, robots de cintas, generadores, ...
instalaciones	recinto, edificio, sala, canalización, vehículo, instalaciones de respaldo, ...
personal	usuarios internos, usuarios externos, operadores, administradores (de red, de sistemas, de BD, de seguridad, ...), desarrolladores, proveedores, subcontratas, ...

También se consideran activos aspectos intangibles como ”reputación”, ”confianza”, ”imagen de marca”, etc

AMENAZAS, RIESGOS y VULNERABILIDADES

INTRODUCCION

- AMENAZA: **la posibilidad de que un sistema vulnerable sea atacado y sufra daños**

- RIESGO: **posibilidad de que un sistema sufra un incidente de seguridad y que una amenaza se materialice causando una serie de daños**

- VULNERABILIDADES: **debilidad propia de un sistema que permite ser atacado y recibir un daño**

1.- RIESGO

- “Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias”.

2.- AMENAZAS

- Las **amenazas no se pueden eliminar**, porque existen de manera intrínseca al contexto y entorno en que existen los equipos informáticos. Por lo tanto, existe la obligación de analizarlas para poder reducir el daño que supondrían en los equipos informáticos.
- Para causar el daño, la amenaza debe encontrar un punto en que afecte al equipo; este punto es una vulnerabilidad del equipo ante la amenaza. Es decir, las vulnerabilidades son **las debilidades de los equipos ante las amenazas.**

Amenazas (1)

Cualquier peligro potencial sobre un activo de la organización

- Algo o alguien que puede aprovechar una vulnerabilidad (explotarla) para causar un impacto sobre la confidencialidad, integridad o disponibilidad de un activo
- Pueden ser accidentales o intencionadas

Tipos de amenazas (según Libro II de la metodología MAGERIT ver. 3)

desastres naturales	fuego, daños por agua, terremotos, derrumbes, caídas, ...
de origen industrial	fuego, daños por agua, contaminación mecánica, contaminación electromagnética, avería física o lógica, corte de suministro eléctrico, temperatura/humedad inadecuada, fallo de comunicaciones, interrupción de servicios y suministros esenciales, degradación de soportes almacenamiento, ...
errores y fallos no intencionados	errores de usuarios, errores de administrador, errores de monitorización, errores de configuración, deficiencias en la organización, difusión de software dañino, escapes de información,alteración accidental de la información, destrucción de la información, fugas de información, vulnerabilidades del software, errores de mantenimiento/actualización del software, errores de mantenimiento o actualización del hardware, caída del sistema por agotamiento de recursos, pérdida de equipos, indisponibilidad del personal, ...
ataques intencionados	manipulación registros de actividad, manipulación de la configuración, suplantación de usuario, abuso de privilegios de acceso, uso no previsto, difusión de software dañino, repudio, acceso no autorizado, análisis de tráfico, interceptación/escucha de información, modificación o destrucción de información, divulgación de información, manipulación de programas, robo manipulación de equipos, denegación de servicio, ataque destructivo, ocupación enemiga, indisponiblidad del personal, extorsión, ingeniería social, ...

Amenazas (2)

Tipos genéricos de amenazas (por su efecto sobre los activos)

de interrupción hacen que un activo del sistema se pierda o quede inutilizado

- atenta contra la disponibilidad

de interceptación un elemento no autorizado tiene acceso a un activo del sistema

- atenta contra la confidencialidad

de modificación además de acceder, el elemento no autorizado consigue modificar el activo

- atenta contra la integridad (y disponibilidad en caso de destrucción)

de fabricación un elemento no autorizado consigue ”construir” una réplica de un activo legítimo

3.- VULNERABILIDADES

- La **vulnerabilidad**, por lo tanto, permite o facilita que una amenaza dañe el equipo; mientras que la amenaza es **cualquier hecho que, intencionadamente o no, aprovecha una vulnerabilidad para dañar un equipo.**

- Por último, cuando una amenaza o un conjunto de ellas sucede, y aprovecha una vulnerabilidad, se dice que ha ocurrido un **incidente de seguridad,** cuyo efecto es un **daño o impacto** al equipo informático.

Vulnerabilidades

Debilidades que pueden proporcionar a una amenaza la posibilidad de comprometer y/o causar daño a un activo

- defectos de diseño o construcción
- deficiencias de configuración
- deficiencias en su instalación o uso, etc
- ausencia de controles de seguridad

Riesgo

Cuantificación de la posibilidad de que una amenaza aproveche una vulnerabilidad causando un impacto en la confidencialidad, integridad o disponibilidad de un activo

- Suele tener asociada una valoración del coste que supone
- Cuantifica: { probabilidad de ocurrencia de la vulnerabilidad + coste del daño potencial sobre el activo

4.- ¿Cómo reducir el riesgo en un sistema?

- **detecten e identifiquen las distintas vulnerabilidades** existentes, **aplicando las acciones necesarias para corregirlas y evitar que las amenazas que representan puedan llegar a materializarse**

- Normalmente, las amenazas serán genéricas, y no se podrán eliminar por completo, mientras que las vulnerabilidades serán particulares de cada equipo, y sí permiten intervenir en ellas.

- Frente a los incidentes de seguridad, se deben disponer **contramedidas o salvaguardas** que fortalezcan el sistema. Las contramedidas persiguen **conocer, prevenir, impedir, reducir y controlar el daño** que podría tener un equipo.

Mecanismos/controles de seguridad (1)

Elementos físicos, técnicos o organizativos que permiten mitigar un riesgo potencial

- También: contramedidas, salvaguardas, ...
- **Reducen el riesgo** sobre uno o varios activos
  - eliminando la vulnerabilidad de lo causa
  - reduciendo la posibilidad de que la vulnerabilidad sea explotada

  (también es posible transferir el riesgo a un tercero [contratando un seguro])

Clasificación genérica

- controles **administrativos**: procedimientos, políticas, normas, etc
- controles **técnicos** (lógicos): cortafuegos, cifrado, antimalware, etc
- controles **físicos**: sistemas antiincendios, vigilancia, cerraduras, biometría, etc

Mecanismos/controles de seguridad (2)

Tipos de controles por su funcionalidad

- **preventivos:** pretenden evitar que un incidente de seguridad llegue a ocurrir
- **de detección:** permiten identificar las actividades propias de un incidente de seguridad que está siendo desencadenado por parte de un atacante/amenaza
- **de recuperación:** buscan devolver el sistema a un estado que permita su operación normal
- **correctivos:** corrigen los componentes, sistemas o controles que no han cumplido su labor (una vez que un incidente ya ha sucedido) para evitar futuros incidentes similares
- **disuasorios:** buscan disuadir a los posibles atacantes/amenazas

Ejemplos de tipos de controles

Seguridad física (controles de seg. físicos)	**Seguridad lógica** (controles de seg. técnicos)	**Seguridad organizativa y legal** (controles organizativos y legales)
Preventivos cerraduras tarjetas de acceso control biométrico guardias de seguridad bloqueo de ventanas hacia el exterior normativas de acceso a activos físicos formación de usuarios **De detección** detectores de movimiento cámaras de circuito cerrado detectores de humo **Disuasorios** vallas de seguridad **De recuperación** réplica de activos en otra localización extinción automática	**Preventivos** config. routers (reglas de filtrado) firewalls cifrado de la inform. en tránsito cifrado de la inform. almacenada software antivirus/antimalware **De detección** sistemas detección intrusiones análisis de logs **De recuperación** sistemas y políticas de back-up **Correctivos** réplicas (imágenes) de máquinas preconfiguradas	**Preventivos** políticas y procedimientos procedimientos de contratación de personal clasificación y etiquetado de recursos cumplimiento de leyes/normas **De detección** rotación en puestos investigación de actividades **Disuasorios** sanciones y penalizaciones acuerdos de confidencialidad

Controles del Libro II de Magerit versión 3

Protecciones generales u horizontales
- Identificación y autenticación
- Control de acceso lógico
- Segregación de tareas
- Gestión de incidencias
- Herramientas de seguridad
- Herramienta contra código dañino
- IDS/IPS: Herramienta de detección y prevención de intrusión
- Herramienta de chequeo de configuración
- Herramienta de análisis de vulnerabilidades
- Herramienta de monitorización de tráfico
- Herramienta de monitorización de contenidos
- Herramienta para análisis de logs
- Honey net / honey pot
- Verificación de las funciones de seguridad
- Gestión de vulnerabilidades
- Registro y auditoría

Protección de las aplicaciones (software)
- Copias de seguridad (backup)
- Puesta en producción
- Se aplican perfiles de seguridad
- Explotación / Producción
- Cambios (actualizaciones y mantenimiento)
- Terminación

Protección de los equipos (hardware)
- Protección de los Equipos Informáticos
- Puesta en producción
- Se aplican perfiles de seguridad
- Aseguramiento de la disponibilidad
- Operación
- Cambios (actualizaciones y mantenimiento)
- Terminación
- Informática móvil
- Reproducción de documentos
- Protección de la centralita telefónica (PABX)

Seguridad física – Protección de las instalaciones
- Protección de las instalaciones
- Diseño
- Defensa en profundidad
- Control de los accesos físicos
- Aseguramiento de la disponibilidad
- Terminación

Protección de los datos / información
- Copias de seguridad de los datos (backup)
- Aseguramiento de la integridad
- Cifrado de la información
- Uso de firmas electrónicas
- Uso de servicios de fechado electrónico (time stamping)

Protección de las claves criptográficas
- Gestión de claves criptográficas
- Gestión de claves de cifra de información
- Gestión de claves de firma de información
- Gestión de claves para contenedores criptográficos
- Gestión de claves de comunicaciones
- Gestión de certificados

Protección de las comunicaciones
- Entrada en servicio
- Se aplican perfiles de seguridad
- Aseguramiento de la disponibilidad
- Autenticación del canal
- Protección de la integridad de los datos intercambiados
- Protección criptográfica de la confidencialidad de los datos intercambiados
- Operación
- Cambios (actualizaciones y mantenimiento)
- Terminación
- Seguridad Wireless (WiFi)
- Telefonía móvil
- Segregación de las redes en dominios

Continuidad de operaciones
- Prevención y reacción frente a desastres.
- Continuidad del negocio
- Análisis de impacto (BIA)
- Recuperación de Desastres (DRP)

Adquisición y desarrollo
- Adquisición / desarrollo
- Servicios: Adquisición o desarrollo
- Aplicaciones: Adquisición o desarrollo
- Equipos: Adquisición o desarrollo
- Comunicaciones: Adquisición o contratación
- Soportes de información: Adquisición
- Productos certificados o acreditados

Salvaguardas de tipo organizativo
- Organización
- Gestión de riesgos
- Planificación de la seguridad
- Inspecciones de seguridad

Protección de los servicios
- Aseguramiento de la disponibilidad
- Aceptación y puesta en operación
- Se aplican perfiles de seguridad
- Explotación
- Gestión de cambios (mejoras y sustituciones)
- Terminación
- Protección de servicios y aplicaciones web
- Protección del correo electrónico
- Protección del directorio
- Protección del servidor de nombres de dominio (DNS)
- Voz sobre IP

Protección en los puntos de interconexión con otros sistemas
- Puntos de interconexión: conexiones entre zonas de confianza
- Sistema de protección perimetral
- Protección de los equipos de frontera

Protección de los soportes de información
- Protección de los Soportes de Información
- Aseguramiento de la disponibilidad
- Protección criptográfica del contenido
- Limpieza de contenidos
- Destrucción de soportes

Protección de los elementos auxiliares
- Aseguramiento de la disponibilidad
- Instalación
- Suministro eléctrico
- Climatización
- Protección del cableado

Externalización
- SLA: nivel de servicio, si la disponibilidad es un valor
- NDA: compromiso de secreto, si la confidencialidad es un valor
- Identificación y calificación del personal encargado
- Procedimientos de escalado y resolución de incidencias
- Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)
- Asunción de responsabilidades y penalizaciones por incumplimiento
- Acuerdos para intercambio de información y software
- Acceso externo
- Servicios proporcionados por otras organizaciones
- Personal subcontratado

Salvaguardas relativas al personal
- Gestión del Personal
- Formación y concienciación
- Aseguramiento de la disponibilidad

Ejemplo

Activo:	PCs de una organización
Amenaza:	Nuevo virus/malware (no reconocido por el software antivirus)
Vulnerabilidad:	Firmas de virus no actualizadas en el antivirus corporativo
Riego:	Posibilidad de que esos virus no reconocidos infecten los equipos y causen daños/pérdidas Supondrá cuantificar: - probabilidad de que suceda la infección - coste que supondría la infección, incluyendo * coste por posible pérdida/robo de datos * coste de las molestias y pérdida de tiempo productivo de los usuarios * coste de la eliminación del virus o la reinstalación de equipos * otros costes
Contramedidas:	técnicas: - programar actualización del antivirus (adquiriéndolas si es preciso o cambiando de antivirus) organizativas: - definir criterios para selección y compra de antivirus - definir procedimientos de instalación y actualización de antivirus - establecer políticas de concienciación de usuarios

6.- MEDIDAS

- Realizar una **auditoría** de seguridad para identificar las vulnerabilidades y establecer las amenazas que representan para los sistemas y la información.
- Aplicar las medidas para eliminar las vulnerabilidades (actualización de sistemas operativos y programas informáticos o aplicación de parches de seguridad).
- Invertir en formación del personal en ciberseguridad para eliminar los errores humanos relacionados con la seguridad, fomentando las mejores prácticas.
- Establecer protocolos de actuación en el caso de que una amenaza finalmente se materialice.

6.1 MEDIDAS

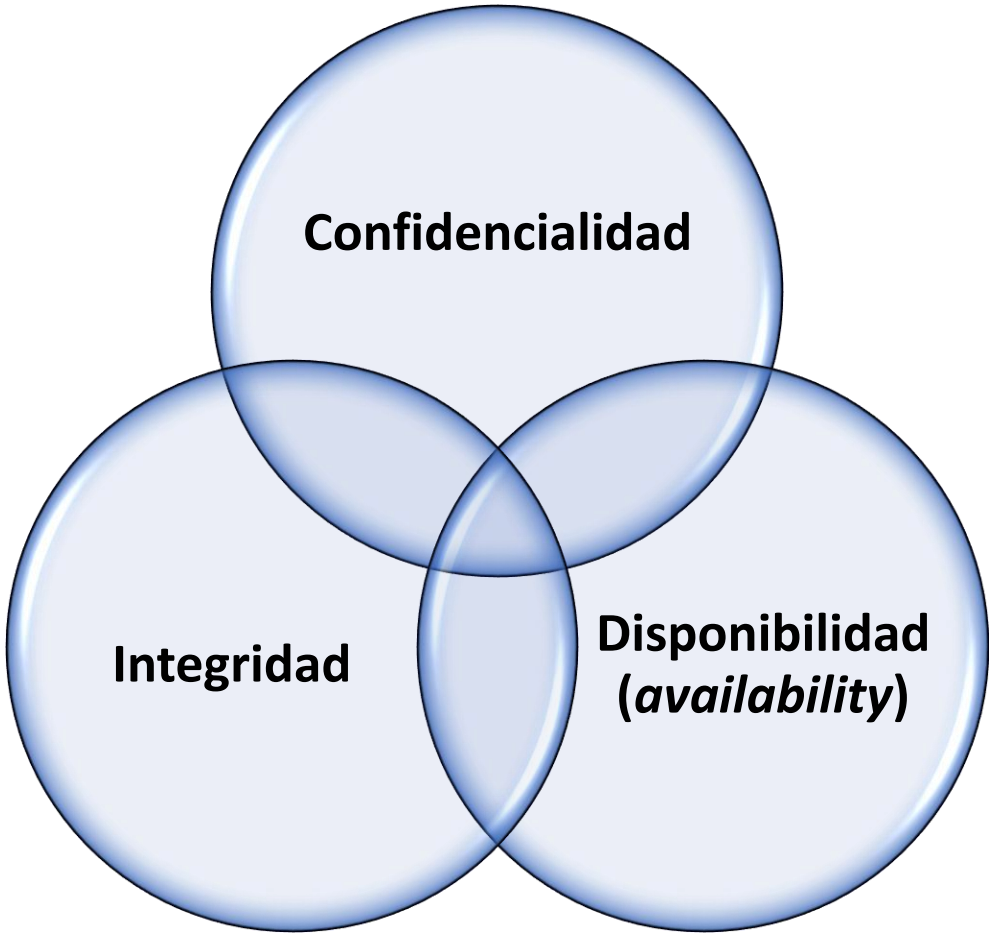
- Definir una **política de seguridad clara y concisa**, y hacerla pública para que todo el personal la conozca a fondo y pueda cumplirla (no utilizar dispositivos personales para conectar a la red empresarial o reglas de creación de password seguras).
- Se debe integrar el concepto de seguridad en todos los procesos y tareas de la empresa. Cada acción o actividad que se realice en el negocio debe evaluar sus vulnerabilidades y establecer a qué amenazadas se expone, para así reducir el riesgo de que se produzcan.
- Utilizar herramientas de protección como firewalls, programas antimalware, sistemas de doble autenticación y consolas de seguridad cloud, entre otros.

6.2 MEDIDAS

- Utilizar **herramientas de monitorización de seguridad** para detectar amenazas y poder reaccionar de forma inmediata para evitarlas o reducir su impacto.
- Llevar un sistema de registro y documentación de toda la actividad relacionada con la seguridad, como incidencias de seguridad, intervenciones realizadas, protocolos de actuación, etc.
- Apostar por proveedores de servicios cloud con un alto nivel de seguridad, que cuenten con las certificaciones y credenciales de seguridad aceptadas como estándares a nivel mundial.

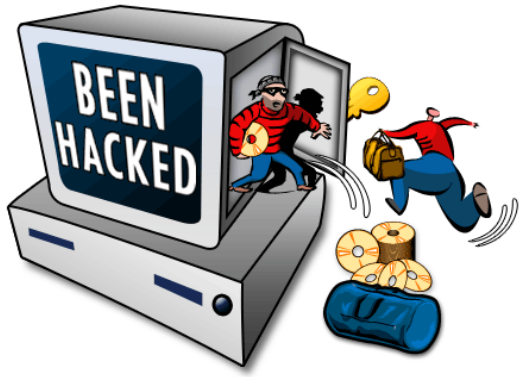
PRINCIPIOS DE SEGURIDAD

El trío CIA


Confidencialidad
Integridad
Disponibilidad
(*availability*)

Confidencialidad

- Preservar las restricciones de autorización para acceso y revelado de información, incluyendo medios para proteger la privacidad personal e información propietaria
- La pérdida de confidencialidad implica el acceso o revelado no autorizado de información
- Incluye:
  - **Confidencialidad de datos** (información): asegura que los datos privados no sean hechos públicos o revelados a personas no autorizadas
  - **Privacidad**: asegura que cada individuo controla y decide qué información (sobre él mismo) puede ser recogida y almacenada y por quién, y a quién puede ser revelada



Confidencialidad

- Ejemplo: Ana y Pedro quieren que su comunicación sea un secreto para Eva

- Clave (key): secreto compartido entre Ana y Pedro

- Algunas veces se consigue con
  - Criptografía
  - Esteganografía
  - Control de acceso
  - Vistas en las BB.DD.

Integridad

- Evitar modificaciones o destrucción no apropiada de los datos, incluyendo asegurar el no-rechazo (*non-repudiation*) y autenticidad de los datos
- Integridad de datos = datos no corruptos
- La pérdida de integridad significa la modificación o destrucción no autorizada de los datos
- Incluye:
  - **Integridad de datos**: asegurar que la información y los programas son modificados sólo de forma específica y autorizada
  - **Integridad del sistema**: asegurar que un sistema ejecuta la funcionalidad prevista sin menoscabo, sin manipulación no autorizada (sea con o sin intención)

Integridad

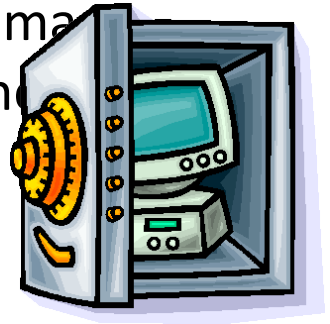
- Ejemplo:
  - Ataque de hombre en el medio (*Man in the middle attack - MITM*)
    - ¿Ha manipulado Mallory el mensaje que Alice le mandó a Bob?

- Verificación de integridad: agregar redundancia a los datos/mensajes

- Técnicas:
  - Hashing, Checksums (CRC,…)
    - Ojo al uso de algoritmos obsoletos, p.ej., MD5, SHA-1,…
  - Códigos de Autenticación de mensajes (MACs)
    - Basados en claves

Disponibilidad

- Asegurar que la información pueda ser accedida y utilizada de forma confiable y en tiempo
- La pérdida de disponibilidad significa la interrupción o demora de acceso o uso de la información o sistema de información a usuarios legítimos
- Cómo:
  - Agregar redundancia para evitar un punto único de falla
  - Imponer límites a lo que los usuarios legítimos pueden hacer
- El objetivo de los ataques (distribuidos) de denegación de servicios ((D)DOS) es reducir la disponibilidad
  - Se utiliza malware para enviar un tráfico excesivo al servidor víctima
  - Servidores saturados (sobrepasados) no pueden atender peticiones



Objetivos adicionales

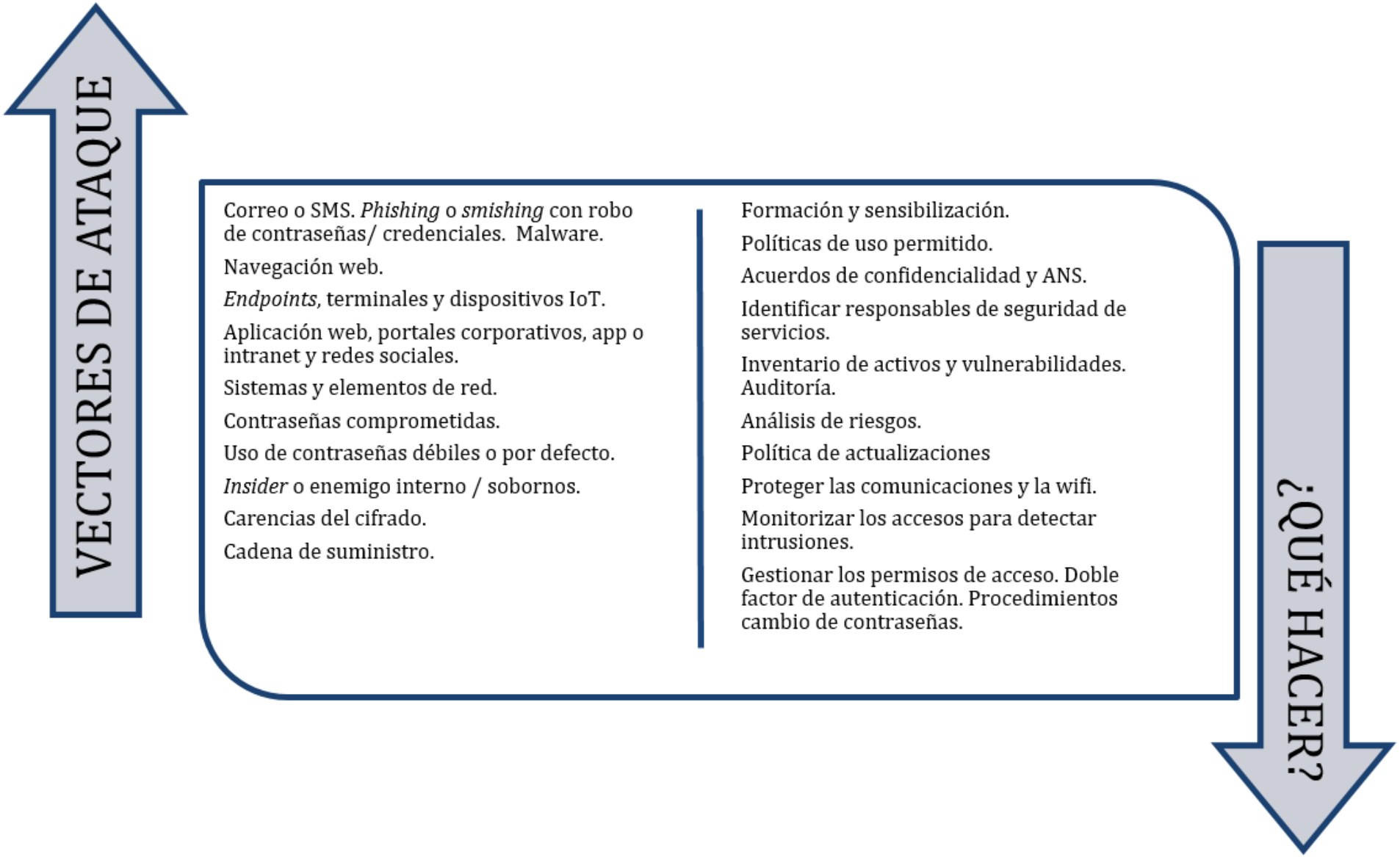
- **Autenticidad**:
  - Propiedad de ser genuino y capaz de ser verificado y confiable; confianza en la validez de una transmisión, mensaje u origen de un mensaje
  - Implica verificar que los usuarios son quienes dicen ser y que cada entrada al sistema viene de una fuente de confianza
- **Asignación de responsabilidad** (accountability): que las acciones de una entidad puedan ser atribuidas de forma unívoca a esa entidad
  - Porque el sistema realmente seguro no existe, debe ser posible atribuir responsabilidades de intrusiones

La seguridad desde el diseño

- Diseñar el sistema con la seguridad en mente
  - No puede ser una idea posterior (ah! y ahora vamos a controlar…)
  - Difícil “agregar” seguridad *a posteriori*
- Definir objetivos de seguridad concretos y medibles
  - Sólo algunos usuarios pueden ejecutar X. Registrar la acción
  - La salida de la función Y debe ser encriptada
  - La función Z debe estar disponible el 99% del tiempo

- Dos conceptos fundamentales a día de hoy en el diseño de sistemas informáticos:
  - *Pentesting*
  - Análisis forense

Vectores de ataque



TIPOS DE SEGURIDAD

La seguridad es holística

- Seguridad física.
- Seguridad tecnológica
  - Seguridad de la aplicación.
  - Seguridad del sistema operativo.
  - Seguridad de la red
- Políticas y procedimientos.

- Las tres partes son necesarias

1.- Seguridad física

- Limitar el acceso al espacio físico para prevenir robo de bienes y entradas no autorizadas.
- Protección contra filtrado de información y robo de documentos.
- Ejemplo: *Dumpster Diving*: recolectar información sensible revisando la basura de la empresa víctima

2.- Seguridad de la aplicación

- Ejemplo: navegador y servidor Web.

- Un correcto proceso de verificación de identidad.
- Correcta configuración del servidor:
  - Ficheros locales.
  - Contenidos de la base de datos.
- Interpretación robusta de los datos.

3.- Seguridad de S.O. y red

- Las aplicaciones usan el S.O. para muchas funciones.
- El código del S.O. a menudo contiene vulnerabilidades.
  - Actualizaciones frecuentes.
- Seguridad de la red: mitigar el tráfico malicioso.
- Herramientas: cortafuegos y sistemas de detección de intrusiones.

4.- Políticas y Procedimientos

- Ejemplo: ataque de ingeniería social – aprovecharse de empleados desprevenidos (es decir, los atacantes logran que un empleado divulgue su usuario y clave).

- Custodiar la información empresarial sensible.

- Los empleados deben estar prevenidos, ser entrenados para ser un poco paranoicos y estar vigilantes.

¿CÓMO PROTEGERNOS?

2. SEGURIDAD DE EQUIPOS INFORMÁTICOS

- ¿Cómo nos infectan?
- ¿Qué puede pasar?
- Si nos han infectado ¿Cómo podemos recuperar la información?
- ¿Qué puedo hacer para minimizar los riesgos?

INFECCIÓN DE NUESTROS EQUIPOS

¿POR QUÉ LO HACEN?

- Instalar MALWARE
- Robar información personal o profesional
- Robar dinero

CÓMO SE INFECTAN NUESTROS EQUIPOS (I)

CORREO ELECTRÓNICO

- **Fichero adjunto**, suele tratarse de un programa ejecutable (.exe), un fichero PDF o un fichero comprimido (.zip o .rar).

- **Links que redirigen a una web** maliciosa que contiene malware para infectarnos o que simula ser un servicio real.

¿CÓMO DETECTO UN EMAIL FRAUDULENTO?

- Tiene documentos adjuntos ejecutables
- Redacción incorrecta
- Enlaces falsos
- Solicitan información de tarjetas de crédito
- Otros:
  - Páginas de ofertas de trabajo, préstamos, página de contactos, etc.

TIPOS DE INFECCIÓN

RANSOMWARE:
"Secuestra" el ordenador, smartphone o los ficheros que contiene, pidiendo un "rescate" para permitirnos usar de nuevo el dispositivo o que podamos recuperar los ficheros.

PHISHING:
Suplantación de la identidad de un banco, operadora, organismo oficial, compañía eléctrica para robarle información privada.

RANSOMWARE: EJEMPLOS REALES

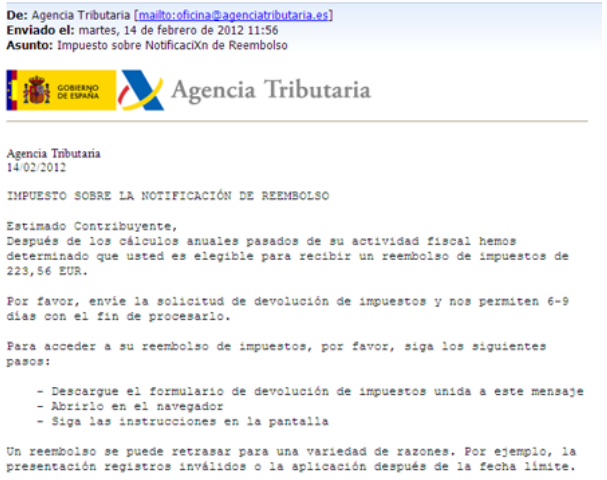
- Ha aumentado un 128% el último año
- Algunos han infectado a 10.000 usuarios en 15 días

RANSOMWARE

1. **Bloquea los ficheros**: el disco duro trabaja de forma ininterrumpida hasta que cifre todos los ficheros de usuario.
2. **Cifra** más de 120 extensiones de archivos de usuario (doc, xls, jpg, mp3, avi…).
3. Al final, nos muestra un **mensaje** en el que se indica lo que ha pasado.

RANSOMWARE: EJEMPLOS REALES (II)

PHISHING: EJEMPLOS REALES



De: Agencia Tributaria [mailto:oficina@agenciatributaria.es]
Enviado el: martes, 14 de febrero de 2012 11:56
Asunto: Impuesto sobre NotificaciXn de Reembolso

GOBIERNO DE ESPAÑA — Agencia Tributaria

Agencia Tributaria
14/02/2012

IMPUESTO SOBRE LA NOTIFICACIÓN DE REEMBOLSO

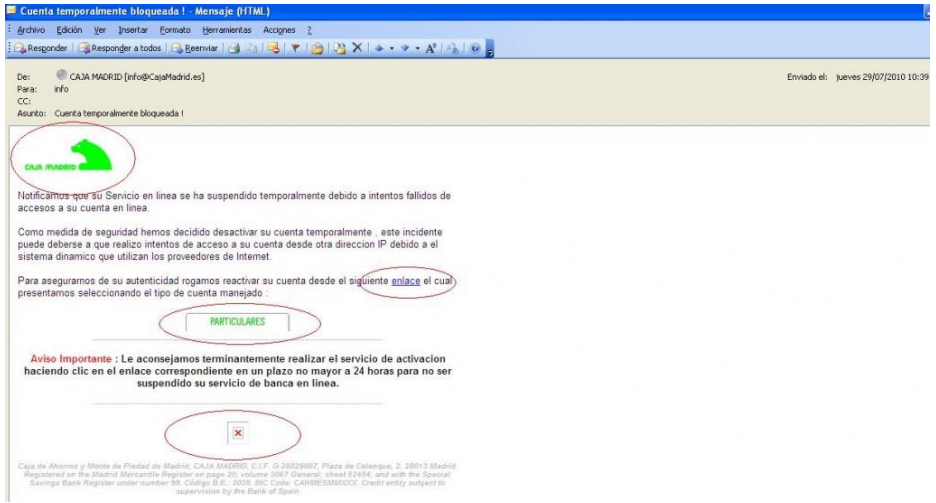
Estimado Contribuyente,
Después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 EUR.

Por favor, envíe la solicitud de devolución de impuestos y nos permiten 6-9 días con el fin de procesarlo.

Para acceder a su reembolso de impuestos, por favor, siga los siguientes pasos:

- Descargue el formulario de devolución de impuestos unida a este mensaje
- Abrirlo en el navegador
- Siga las instrucciones en la pantalla

Un reembolso se puede retrasar para una variedad de razones. Por ejemplo, la presentación registros inválidos o la aplicación después de la fecha límite.



Cuenta temporalmente bloqueada ! - Mensaje (HTML)

Archivo Edición Ver Insertar Formato Herramientas Acciones ?

Responder | Responder a todos | Reenviar

De: CAJA MADRID [info@CajaMadrid.es]
Para: info
CC:
Asunto: Cuenta temporalmente bloqueada !
Enviado el: jueves 29/07/2010 10:39

CAJA MADRID

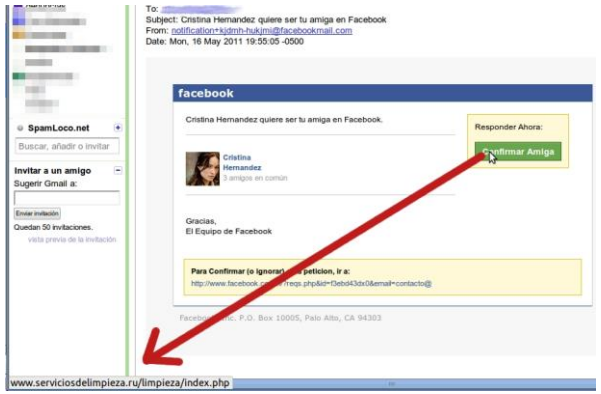
Notificamos que su Servicio en linea se ha suspendido temporalmente debido a intentos fallidos de accesos a su cuenta en linea.

Como medida de seguridad hemos decidido desactivar su cuenta temporalmente , este incidente puede deberse a que realizo intentos de acceso a su cuenta desde otra direccion IP debido a el sistema dinamico que utilizan los proveedores de Internet.

Para asegurarnos de su autenticidad rogamos reactivar su cuenta desde el siguiente enlace el cual presentamos seleccionando el tipo de cuenta manejado :

PARTICULARES

Aviso Importante : Le aconsejamos terminantemente realizar el servicio de activacion haciendo clic en el enlace correspondiente en un plazo no mayor a 24 horas para no ser suspendido su servicio de banca en linea.



To:
Subject: Cristina Hernandez quiere ser tu amiga en Facebook
From: notification+kidmh-hukjmi@facebookmail.com
Date: Mon, 16 May 2011 19:55:05 -0500

SpamLoco.net
Buscar, añadir o invitar
Invitar a un amigo
Sugerir Gmail a:
Enviar invitación
Quedan 50 invitaciones.
vista previa de la invitación

facebook

Cristina Hernandez quiere ser tu amiga en Facebook.

Responder Ahora:
Confirmar Amiga

Cristina Hernandez
3 amigos en común

Gracias,
El Equipo de Facebook

Para Confirmar (o ignorar) esta peticion, ir a:
http://www.facebook.com/reqs.php&id=f3eb043dx0&email=contacto@

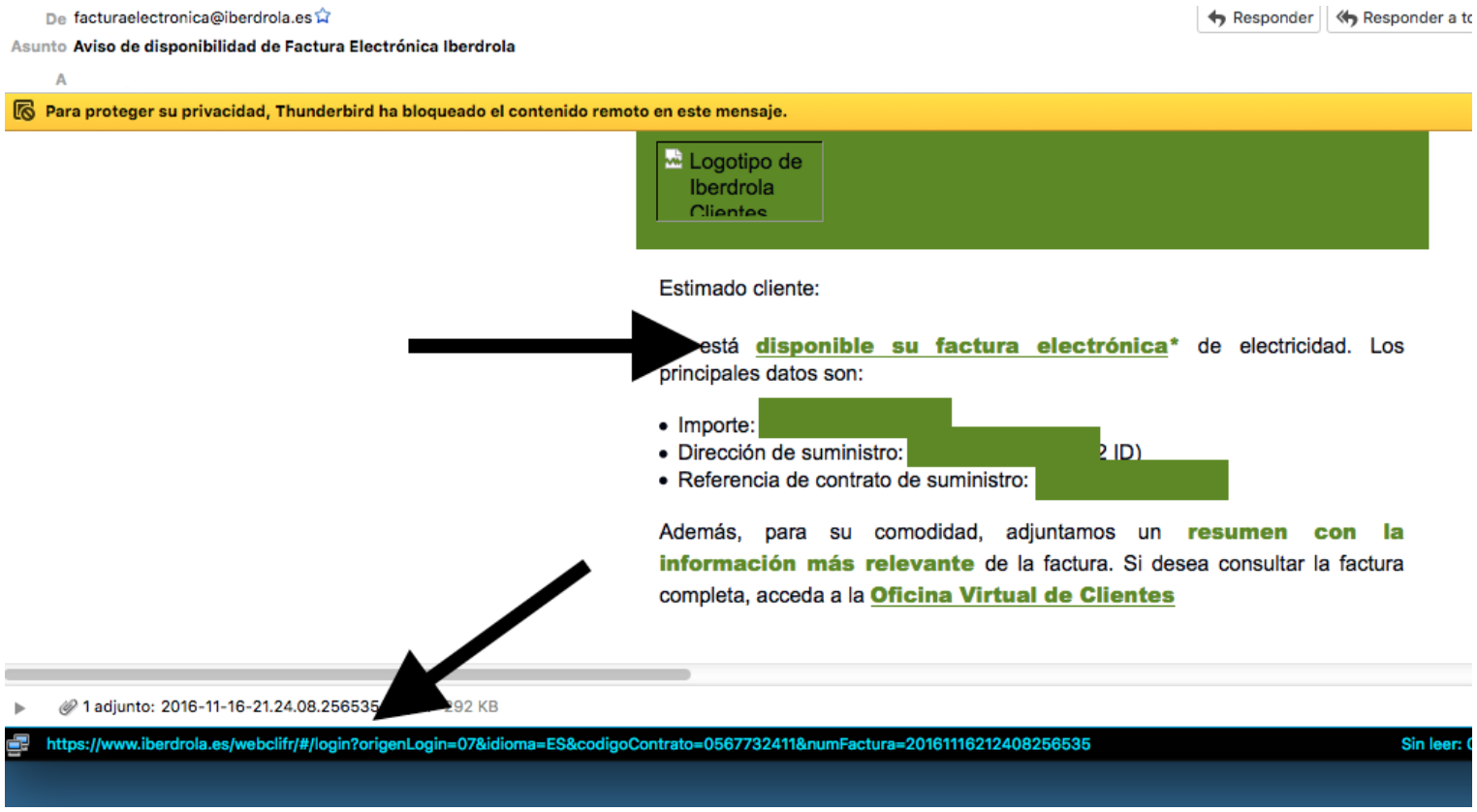
Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

www.serviciosdelimpieza.ru/limpieza/index.php

PHISHING: EJEMPLOS REALES

PHISHING: EJEMPLOS REALES

El email auténtico es así:



AMENAZAS PERSISTENTES AVANZADAS

Advanced Persistent Threats

- Ataque dirigido a un objetivo concreto seleccionado previamente, utilizando técnicas o herramientas elaboradas expresamente para ese objetivo e intentando que la infección se mantenga en el tiempo.

CÓMO SE INFECTAN NUESTROS EQUIPOS (II)

- **Dispositivos de almacenamiento externos**
  - Memorias USB, discos duros, tarjetas de memoria, etc.
- **Descarga de ficheros**
  - Redes P2P o similar
- **Páginas web maliciosas**
  - Problemas de seguridad con el navegador
- **Redes sociales**
  - Enlaces para recoger nuestra información personal
- **Vulnerabilidades / Fallos de seguridad**

CONSECUENCIAS

CONTRAMEDIDAS

1.- Sistema de Autenticación

- Verificar identidad.
- ¿Cómo puede estar A seguro de que se está comunicando con B?
- Existen tres formas generales:
  - Algo que **sabes**: x ejemplo claves.
  - Algo que **tienes**: x ejemplo *tokens*.
  - Algo que **eres**: x ejemplo parámetros biométricos

Algo que *SABES*

- Ejemplo: claves
  - Ventajas:
    - Simple de implementar.
    - Simple de entender para los usuarios.
  - Desventajas:
    - Fácil de romper (a menos que el usuario elija clave fuerte).
    - Las claves se reutilizan muchas veces.
- Claves de usar y tirar (*one time passwords* – OTP): utilizar una clave diferente cada vez.
  - Es difícil para los usuarios recordar todas (apuntarlas?!?!??!)

Algo que *TIENES*

- Tarjetas OTP: generan nueva clave cada vez que el usuario ingresa.
- Tarjeta inteligente (Smart Card):
  - Resistente a la manipulación, almacena información secreta. se inserta en un lector de tarjetas.

- Token / Llave: x ejemplo iButton.
- Tarjeta de cajero automático.
- La fortaleza de la autenticación depende de la dificultad de imitar el producto.

Algo que *ERES*

- Parámetros biométricos
- Ventaja: “eleva el listón”.
- Desventajas:
  - Falsos negativos / falsos positivos.
  - Aceptación social.
  - Gestión de claves

Técnica	Efectividad	Aceptación
Escaneo de Palma	1	6
Escaneo de Iris	2	1
Escaneo de Retina	3	7
Huella digital	4	5
Identificación de Voz	5	3
Reconocimiento Facial	6	4
Dinámica de la firma	7	2