

## CIBERSEGURIDAD





## ÍNDICE

---

OBJETIVO ESPECÍFICO .....	3
INTRODUCCIÓN .....	4
1. PROTECCIÓN AL HARDWARE .....	5
1.1. ACCESO FÍSICO .....	7
1.2. DESASTRES NATURALES .....	9
1.3. ALTERACIONES DEL ENTORNO .....	10
1.4. HERRAMIENTAS DE ATAQUE.....	11
2. SEGURIDAD LÓGICA .....	12
2.1. PROTECCIÓN DE ACCESO A LOS SISTEMAS DE DATOS.....	13
2.1.1. SEGURIDAD INTERNA .....	14
2.1.2. SEGURIDAD EN REDES PERIMETRALES.....	18
2.1.3. BIOMETRÍA .....	21
3. POLÍTICAS DE SEGURIDAD.....	23
COMENTARIO FINAL.....	25
REFERENCIAS.....	26



## OBJETIVO ESPECÍFICO

---

- Identificar la seguridad física y lógica de hardware y software.

## INTRODUCCIÓN

La seguridad de la información abarca los espectros más amplios imaginables, considerando que las empresas manejan información en todo tipo de formatos (en dispositivos de almacenamiento, computadores, impresoras, papel, etc.).

Es por esto que la seguridad de la información no puede estar ajena a la seguridad física de los controles de acceso a las dependencias de una compañía y, con mayor razón, de la seguridad lógica en todos los sistemas informáticos.

Es tal la importancia de este tema para la seguridad de la información, que la normativa ISO 27002, en su apartado 9 “Seguridad física y del entorno”, establece:

Áreas de seguridad:

- Perímetro de seguridad física.
- Controles físicos de entrada.

Seguridad en los equipos computacionales:

- Instalación y protección de equipos.
- Seguridad eléctrica.
- Seguridad en la reutilización de equipos.

Hoy en día, los sistemas de información de acceso físico se encuentran protegidos por sistemas biométricos o de otro tipo para autenticar debidamente a los usuarios. Un ejemplo de ello son las nuevas características de seguridad incorporadas en la nueva cédula de identidad emitida por el Registro Civil.

“

Si piensas que vales lo que sabes, estás muy equivocado. Tus conocimientos de hoy no tienen mucho valor más allá de un par de años. Lo que vales es lo que puedes llegar a aprender, la facilidad con la que te adaptas a los cambios que esta profesión nos regala tan frecuentemente.

”

José M. Aguilar

## 1. PROTECCIÓN AL HARDWARE

La seguridad física consiste, tal y como su propio nombre indica, en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor de los sistemas de información, así como a los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

El hardware es frecuentemente el elemento más costoso de todo sistema informático y, por lo tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Figura 1. Esquema de los problemas de seguridad física en una organización



Si alguien que deseara atacar un sistema tuviera acceso físico al mismo, todo el resto de medidas de seguridad implantadas se convertirían en inútiles. De hecho, muchos ataques son entonces triviales, como por ejemplo los de denegación de servicio; si se apaga una máquina que proporciona un servicio es evidente que nadie podrá utilizarlo. Otros ataques se simplifican enormemente. Por ejemplo, si se deseara obtener datos, se podrían copiar los ficheros o robar directamente los discos que los contienen. Incluso, dependiendo del grado de vulnerabilidad del



sistema, sería posible tomar el control total del mismo, por ejemplo, reiniciándolo con un disco de recuperación que permitiera cambiar las claves de los usuarios. Este último tipo de ataque es un ejemplo claro de que la seguridad de todos los equipos es importante, generalmente si se controla el PC de un usuario autorizado de la red es mucho más sencillo atacar otros equipos de la misma.

Para evitar todo este tipo de problemas, se deberá implantar mecanismos de prevención (control de acceso a los recursos) y de detección (si un mecanismo de prevención falla, o no existe, se debería al menos detectar los accesos no autorizados cuanto antes).

Conocido es el caso del Samsung Galaxy Note 7, que en 2016 reportó una falla en la batería, generando múltiples casos en los que el equipo explotó y se encendió en llamas estando conectado al cargador o sencillamente encendido. En total, la empresa calculó que habría 2,5 millones de celulares afectados y los llamó a revisión para repararlos.

Figura 2. Samsung Galaxy Note 7, quemado por falla de hardware.



Fuente: <https://goo.gl/DqxHLD>

Recientemente se descubrieron dos vulnerabilidades graves que afectan a los procesadores de dispositivos de comunicación, denominados Meltdown y Spectre, las que han afectado a buena parte del mundo, por lo que todo tipo de compañías han tenido que ponerse en marcha para reparar las vulnerabilidades en sus productos. Estos problemas afectan a todos los procesadores modernos y a casi todos los sistemas operativos: Windows, Linux, Android, iOS, macOS, FreeBSD, etc. Por otro lado, es extensible a teléfonos inteligentes y otros dispositivos fabricados en los últimos 20 años. Así, Spectre y Meltdown son los nombres de las vulnerabilidades detectadas en muchos procesadores de Intel, ARM y AMD, que podrían permitir a los atacantes robar contraseñas, claves de cifrado y todo tipo de información privada.

Afortunadamente los diferentes fabricantes ya están liberando actualizaciones para la protección del hardware en los diferentes sistemas operativos.

## ENLACE DE INTERÉS

Luego de la catástrofe que significó la existencia de Spectre y Meltdown, las entidades más afectadas por la situación han tenido que reaccionar rápidamente probando y aplicando los parches respectivos lanzados por Intel y Microsoft.

<https://www.fayerwayer.com/2018/01/parches-meltdown-spectre/>



### 1.1. ACCESO FÍSICO

El principal objetivo de la seguridad de acceso física es proteger la información (confidencialidad, integridad y disponibilidad - CIA) de amenazas propias del mundo físico, tales como:

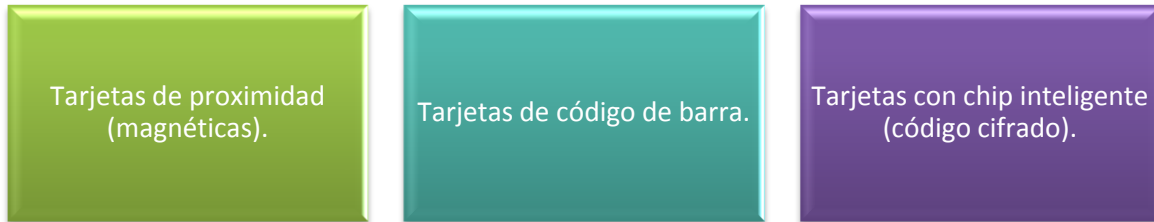
- **Acceso de personas no autorizadas:** que corresponde al ingreso no autorizado de personas a una organización
- **Desastres naturales:** se refiere a algún desastre natural que pueda causar pérdida de la información como incendios, terremotos, etc.
- **Robos:** se refiere a la pérdida de algún activo de información como computadores, libros contables, etc.

Principales  
controles  
físicos  
usados en  
las  
compañías

- Controles de acceso.
- Torniquetes.
- Cerradura con huella digital.
- Fotocopia.
- Circuito cerrado de televisión (CCTV).



Uno de los principales controles que se aplican a los sistemas de acceso físico son las tarjetas de acceso, de las cuales existen de diferentes tipos. Su principal objetivo es identificar al usuario cuando accede a un área restringida, como por ejemplo:

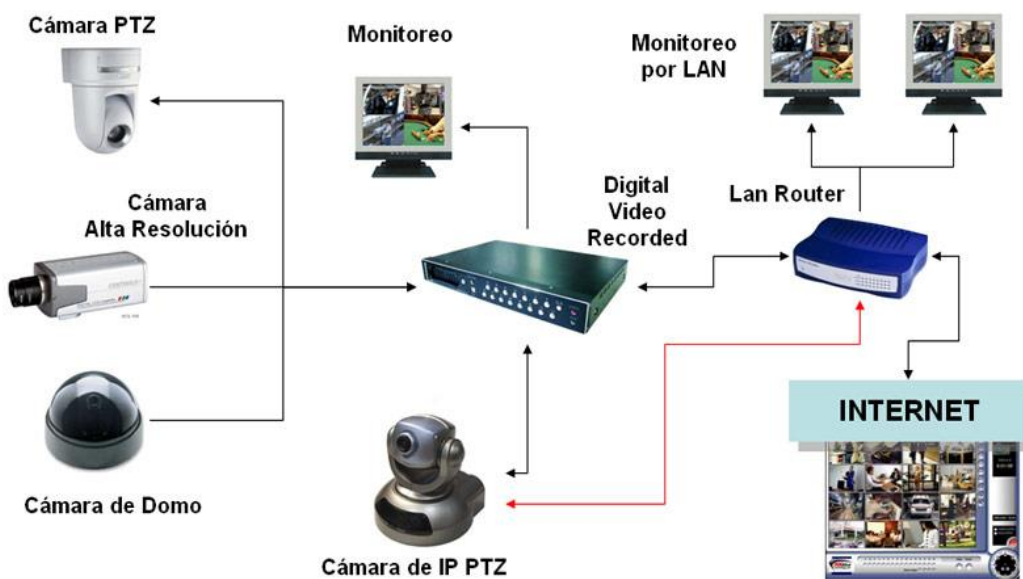


Las principales amenazas para este tipo de controles de seguridad física serían:

- **Tailgating:** cuando un usuario no autorizado ingresa aprovechando el acceso de un usuario autorizado.
- **Suplantación:** robo de tarjetas de acceso.

El control circuito cerrado de TV (CCTV) es una tecnología que permite grabar en señal de video, análoga o digital, los eventos en ambientes controlados. Su principal objetivo es detectar, identificar y registrar accesos y salidas no autorizados.

Figura 3. Esquema de un sistema de seguridad de circuito cerrado de TV



Fuente: <http://blog.todoelectronica.com/tipos-camaras-de-vigilancia-seguridad-escoger/>





Dicho sistema de circuito cerrado de TV permite, además, la integración con otros sistemas de seguridad física, tales como:

- Alarmas.
- Cierres de puertas automáticos.
- Grabación por movimiento (sonido).

Las principales amenazas que enfrentan este tipo de controles son:

- Baja resolución.
- Luminosidad.
- Espacio en disco muy utilizado en la actualidad es el circuito cerrado de televisión.

## 1.2. DESASTRES NATURALES

Se alude a cualquier desastre o contingencia al referirse a la interrupción de la capacidad del acceso a la información y procesamiento de esta a través de computadores necesarios para la operación normal de un negocio. Tienen su origen en las fuerzas de la naturaleza y no solo afectan a la información contenida en los sistemas, sino que también representan una amenaza a la integridad de todo el sistema (infraestructura, instalación, componentes, equipos, etc.).

Los principales desastres naturales que pueden afectar a los sistemas de información son:

- **Incendios:** el fuego es considerado el enemigo número uno de las computadoras, ya que puede destruir fácilmente los archivos de información y programas. Aunque los sistemas antifuego pueden detener el avance del siniestro, también pueden causar igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.
- **Inundaciones:** esta es una de las causas de mayores desastres en centros de cómputos. Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje (ya sea natural o artificial).
- **Condiciones climatológicas:** normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada. Por otro lado, las tormentas electromagnéticas y las lluvias



torrenciales con nubarrones pueden causar atenuación en las redes inalámbricas, lo que podrá conducir a la pérdida de datos.

- **Señales de radar:** los resultados de las investigaciones más recientes sobre la incidencia de las señales o rayos de radar en el funcionamiento de un computador demuestran que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor. Ello podría ocurrir solo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.

Como es sabido, los desastres naturales no se pueden prevenir, solo queda estar preparado para evitar pérdidas de información en caso de que ocurran, tales como tener respaldos actualizados, contingencia de alimentación eléctrica, etc.

### 1.3. ALTERACIONES DEL ENTORNO

En cualquier entorno de trabajo hay factores que pueden sufrir variaciones que afectarían a los sistemas y que tendrán que conocerse e intentar controlar. Se deberá contemplar problemas que pueden afectar al régimen de funcionamiento habitual de las máquinas como la alimentación eléctrica, el ruido eléctrico producido por los equipos o los cambios bruscos de temperatura.

Entre los más comunes se encuentran:

- **Electricidad:** quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimentan los equipos; como por ejemplo los cortocircuitos, picos de tensión, cortes de flujo, etc. Para corregir los problemas con las subidas de tensión, se podría instalar tomas de tierra o filtros reguladores de tensión.

Para los cortes, se podrían emplear sistemas de alimentación ininterrumpida (UPS), que además de proteger ante cortes mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión. Estos equipos disponen de baterías que permiten mantener varios minutos los aparatos conectados a ellos, posibilitando que los sistemas se apaguen de forma ordenada (generalmente disponen de algún mecanismo para comunicarse con los servidores y avisar de que se ha caído la línea o de que se ha restaurado después de una caída).

- **Ruido eléctrico:** el ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también por otros ordenadores o por multitud de aparatos, y se transmite a través del espacio o de líneas eléctricas cercanas a la instalación.

Para prevenir los problemas que puede causar el ruido eléctrico, lo más barato es intentar no situar el hardware cerca de los elementos que pueden causar el ruido. En caso de que fuese necesario hacerlo, siempre se podría instalar filtros o apantallar las cajas de los equipos.

- **Temperaturas extremas:** no hace falta ser un genio para comprender que las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. En general, es recomendable que los equipos operen entre 10 y 32 grados Celsius. Para controlar la temperatura se emplearían aparatos de aire acondicionado.

## 1.4. HERRAMIENTAS DE ATAQUE

Siguiendo en el análisis de la problemática de seguridad en el mundo físico, cabe destacar que en el último tiempo se han desarrollado una serie de herramientas de ataque a nivel de hardware, entre las que destacan:

- **USB Rubber Ducky:** es una herramienta de inyección de teclas disfrazada como una unidad flash genérico (pendrive USB). Las computadoras lo reconocen como un teclado normal y aceptan cargas útiles de teclado pre programadas a más de 1000 palabras por minuto. Las cargas útiles se elaboran con un lenguaje de scripting simple y se pueden usar para descartar conchas inversas, inyectar binarios, códigos pin de fuerza bruta y muchas otras funciones automatizadas para el probador de penetración y el administrador de sistemas. Desde 2010, el USB Rubber Ducky ha sido un favorito entre los piratas informáticos, pentesters y profesionales de TI. Con orígenes como el primer HID de automatización de TI que usa un tablero de desarrollo incrustado, desde entonces ha crecido hasta convertirse en una plataforma de ataque de inyección comercial completa. El USB Rubber Ducky capturó la imaginación de los piratas informáticos con su lenguaje de scripting simple, hardware formidable y diseño encubierto.

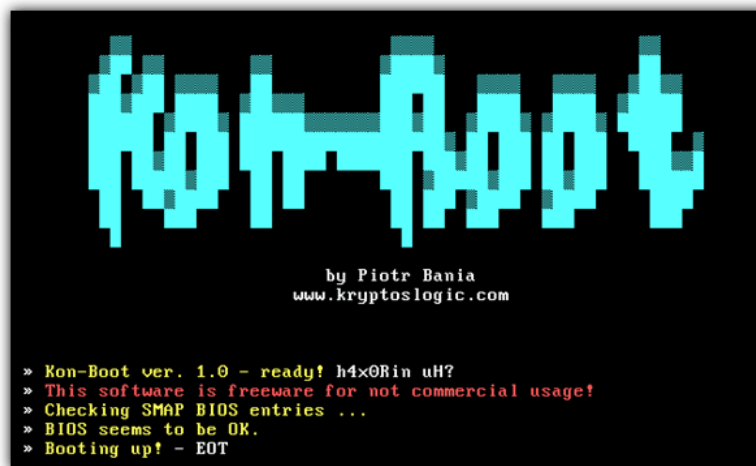
Figura 3. Apariencia del pendrive utilizado por Rubber Ducky



Fuente: <https://goo.gl/ZaK47b>

- **Kon-Boot:** es una aplicación que omitirá silenciosamente el proceso de autenticación de los sistemas operativos basados en Windows, sin sobrescribir su contraseña anterior. En otras palabras, puede iniciar sesión en su perfil de Windows sin conocer su contraseña. Fácil de usar y excelente para reparaciones tecnológicas, recuperación de datos y auditorías de seguridad. También es utilizada por usuarios mal intencionados que buscan conectarse a sistemas de información sin autorización.

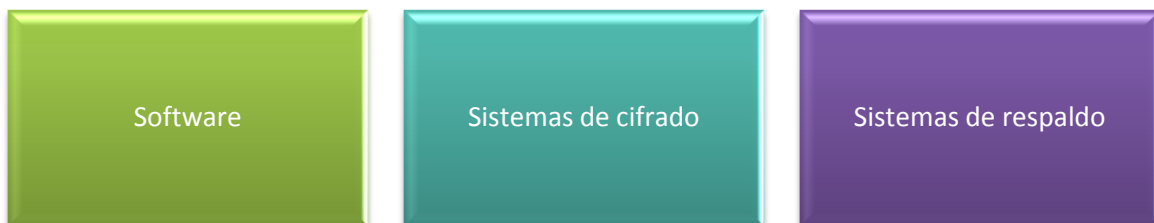
Figura 4. Imagen de inicio de Kon-Boot



Fuente: <https://goo.gl/55mSC6>

## 2. SEGURIDAD LÓGICA

Se refiere a la protección de los activos de información (datos, software, procesos, etc.), resguardando los atributos de la información (CIA) y utilizando como medio o recursos sistemas lógicos de seguridad, tales como:



Los mecanismos de seguridad lógica siguen la siguiente secuencia:

- **Identificación:** es el proceso en el cual un usuario o aplicación valida su identidad a través de algún parámetro.  
  
ID, dirección de mail, nombre de usuario.
- **Autenticación:** es el proceso en el cual se confirma la identidad de un usuario o aplicación a través de un factor que solo él posee.  
  
Contraseña, huella digital, llave privada de cifrado.
- **Autorización:** es el proceso en el cual se le permiten los accesos o derechos en función de su identidad o perfil.
- **Registro:** es el proceso a través del cual se graban las acciones del usuario o aplicación.

Figura 5. Esquema de seguridad lógica.



## 2.1. PROTECCIÓN DE ACCESO A LOS SISTEMAS DE DATOS

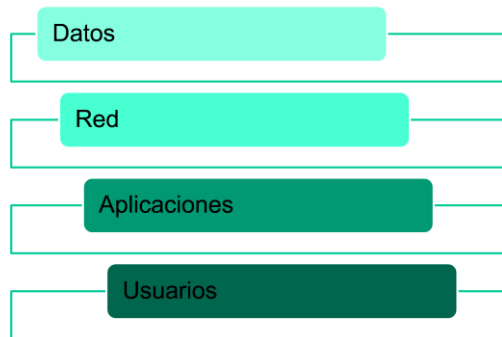
La seguridad lógica, debido a que los controles y amenazas son distintas, se ha dividido, desde el punto de vista de arquitectura de seguridad, en:

### 2.1.1. SEGURIDAD INTERNA

Se refiere al resguardo de los atributos de seguridad de la información de todos los activos que forman parte de la red interna:

- **Bases de datos:** activos donde se almacenan los datos.
- **Servidores de archivos:** activos donde se almacenan archivos para acceso de los usuarios de la organización.
- **Estaciones de trabajo:** activos de uso diario de los usuarios para sus labores organizacionales.

Figura 6. Esquema de seguridad por capas para redes internas



Para proteger estos activos de información es que muchas organizaciones han implementado un “modelo de seguridad por capas”, el cual propone controles de seguridad por cada una de las capas mencionadas a continuación.

- **Datos:** es la capa en la cual se almacena la información, principalmente en bases de datos, servidores de archivos, repositorios.

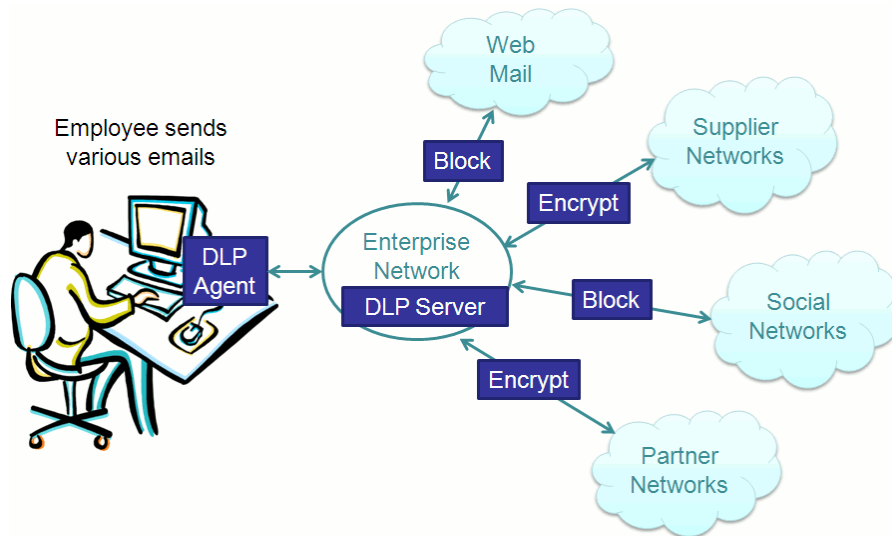
Las principales amenazas de esta capa son:

- Corrupción: alteración no autorizada de los datos.
- Pérdida de datos: borrado de datos.
- Accesos no autorizados: lectura no autorizada de datos.
- Fuga de información: robo de datos.

Los principales controles para estas amenazas son:

- Cifrado en reposo: protección de los datos en sistemas de almacenamiento, tales como bases de datos.
- Scrambling (alteración de los datos): protección de los datos alterando su contenido sin alterar su formato.
- Prevención de fuga de información (Data Loss Prevention).
- Permisos de directorio: acceso a archivos o carpetas restringido por la seguridad del sistema operativo.

Figura 7. Esquema de una solución de prevención de fuga de Información (DLP)



Fuente: <https://goo.gl/PeXKRE>

- **Red:** es la capa a través de la cual se transporta la información desde las aplicaciones hacia los diferentes repositorios.

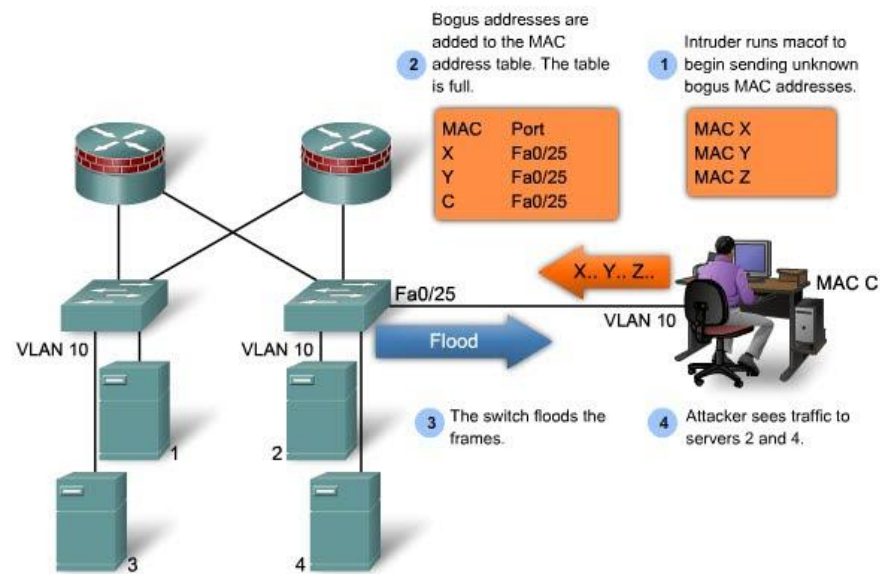
Las principales amenazas de esta capa son:

- Robo de información en tránsito: captura de datos en una transmisión de comunicaciones.
- Acceso a la red no autorizado: capturar datos de una red sin autorización.



- Spoofing ARP o DHCP: suplantación de servicios de red que permiten obtener datos de la red.
- Buffer Overflow: saturación de las capacidades de un switch para robar datos de la red.

Figura 8. Esquema de un ataque de Buffer Overflow de switches de comunicaciones.



Fuente: <https://goo.gl/aYdiBJ>

Los principales controles que operan en la capa de datos son:

- Cifrado de data en tránsito (VPN): permite cifrar la data en tránsito para que no pueda ser capturada por un usuario no autorizado.
- Port Security en switches: permite controlar la cantidad de direcciones MAC soportadas por un switch en cada una de sus interfaces.
- Segmentación: permite aislar un incidente de seguridad.
- **Aplicaciones:** son aquellas que utiliza el usuario para acceder a los datos, donde estas pueden ser:
  - Cliente servidor: aplicaciones que operan con un cliente en la estación del usuario.



- Cliente de base de datos: aplicaciones que permite conexión directa a bases de datos.
- Software de escritorio (Office): aplicaciones para uso habitual de los usuarios.
- Cliente de correo electrónico: aplicación que permite operar con correo electrónico.

Las principales amenazas en la capa de aplicación son:

- Acceso no autorizado a información confidencial.
- Fuga de información.
- Vulnerabilidades en aplicaciones.

Los principales controles utilizados en la capa de aplicación son

- Control de acceso basado en Roles (Role Based Access Control).
- Autenticación robusta.

Por su parte, las empresas utilizan muchos tipos de aplicaciones para acceder a los datos, y estas pueden ser:

- Aplicaciones comerciales.
- Aplicaciones desarrolladas in-house.
- Aplicaciones desarrolladas por terceros.

En general, no se hace una revisión exhaustiva de seguridad a estas aplicaciones ni al tipo de información que manejan, por lo que las principales recomendaciones de seguridad para el manejo de aplicaciones en redes internas serían:

- Revisión de seguridad periódica de las aplicaciones (código y ejecutable).
- Cifrar el tráfico si se maneja información confidencial (SSL o VPN).
- Control de acceso sobre bases de datos.
- No utilizar usuarios genéricos (auditoría).
- No mezclar datos de QA con datos de producción (scrambling).
- Cifrar la data sensible en la base de datos en reposo.
- Sistemas de autenticación robustos para el acceso a aplicaciones (token).



- **Usuarios:** es el encargado de acceder a los datos y, dado que no es posible automatizar controles, es el eslabón más débil de la cadena.

Las principales amenazas que afectan a la capa de usuarios son:

- El usuario no tiene conciencia de la seguridad de la información que maneja.
- El usuario rara vez conoce y aplica las políticas de seguridad.

Los principales controles que se aplican en esta capa no pueden ser tecnológicos, sino que más bien deben estar orientados a capacitar y dotar de competencias a los usuarios:

- Campañas de sensibilización: capacitaciones relacionadas con temáticas de seguridad que afectan a los usuarios.
- Agentes de seguridad locales: usuarios que velan por la seguridad de la información en su piso o departamento.
- Incentivos: premios o reconocimientos de parte de la organización para aquellos usuarios que cumplan las políticas de seguridad.
- Publicaciones permanentes: utilizar la intranet, diario mural, monitores para publicar información relevante de seguridad de los usuarios.

### 2.1.2. SEGURIDAD EN REDES PERIMETRALES

La seguridad perimetral, por su parte, compete a todos los activos que son accesibles desde Internet:

- Red DMZ: conjunto de activos que son accesibles desde Internet.
- Servicios públicos (web, gateway de correo, DNS).
- Enlace y router de internet.

Generalmente, la seguridad de las redes perimetrales o externas se modela a través de los servicios que se publican hacia internet y se generan controles de seguridad particulares para cada uno de ellos. Los principales servicios externos que publican las empresas son:

- Aplicaciones web.
- DNS.
- FTP.
- Gateway de correo electrónico.

Para la seguridad de redes externas, se propone un modelo de seguridad basado en servicios, donde cada aplicación debe tener controles de seguridad específicos de acuerdo con su naturaleza de funcionamiento.

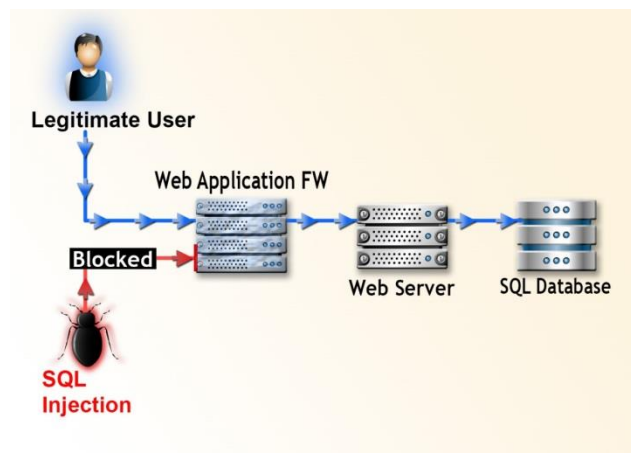
Para las aplicaciones web, las principales amenazas serían:

- Denegación de Servicio (DoS).
- Defacement: cambio no autorizado en las páginas de una aplicación web.
- Robo de información: robo de datos confidenciales.
- Suplantación de identidad: robo de credenciales de un usuario autorizado.
- Fraude (aplicaciones financieras): transacciones realizadas por un tercero no autorizado.
- Vulnerabilidades aplicaciones web.
  - Inyección SQL.
  - XSS.
  - Ejecución de parámetros.

Los principales controles de seguridad utilizados para aplicaciones web son:

- **Firewall aplicativo (WAF - Web Application Firewall):** es un dispositivo hardware o software que permite proteger los servidores de aplicaciones web de determinados ataques específicos en internet. Se controlan las transacciones al servidor web del negocio, lo que básicamente permite evitar, entre otros, los siguientes ataques:
  - Cross-site scripting: consiste en la inclusión de código script malicioso en el cliente que consulta el servidor web.
  - SQL injection: que consiste en introducir un código SQL que vulnere la base de datos del servidor.
  - Denial-of-service: que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

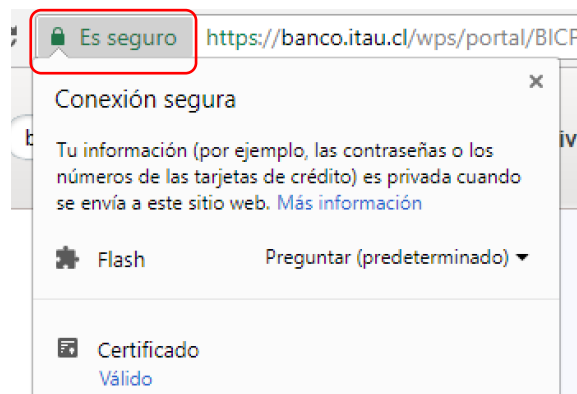
Figura 9. Esquema de operación de un Web Application Firewall (WAF).



Fuente: <https://goo.gl/Dzx8y5>

- **SSL/TLS:** los certificados SSL (capa de sockets seguros) son una pieza esencial de la seguridad de los sitios web. Al visitar un sitio web con SSL, el certificado SSL del sitio permite cifrar los datos que se envían, como la información sobre tarjetas de créditos, nombres y direcciones, de modo que ningún hacker pueda acceder a ellos. Para comprobar si un sitio web usa SSL correctamente, se debe validar que exista el indicador en el browser (típicamente un candado color verde). El protocolo TLS (seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL. Si bien aún se denomina a los certificados de seguridad SSL, es tan solo porque se trata de un término más común. Al comprar certificados SSL en Symantec, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA.

Figura 10. Ejemplo de validación de SSL/TLS



- **Scanning de vulnerabilidades web:** consiste en realizar periódicamente una revisión de vulnerabilidades en las aplicaciones web, de tal forma que se pueda realizar la detección temprana de fallas de seguridad que puedan tener las aplicaciones.
- **Pentesting:** consiste en la explotación controlada de las vulnerabilidades encontradas, con el objetivo de obtener evidencias y confirmar la existencia de dichas vulnerabilidades.

## VIDEO

En el siguiente video se puede revisar una descripción de los principales elementos de red que proveen seguridad al perímetro de una red interna frente a otra que generalmente es internet.

<https://www.youtube.com/watch?v=sxg1nq17xj4>



### 2.1.3. BIOMETRÍA

El origen de la palabra *biometría* está en el griego, donde *metris* significa medición y *bios* vivo o biológico.

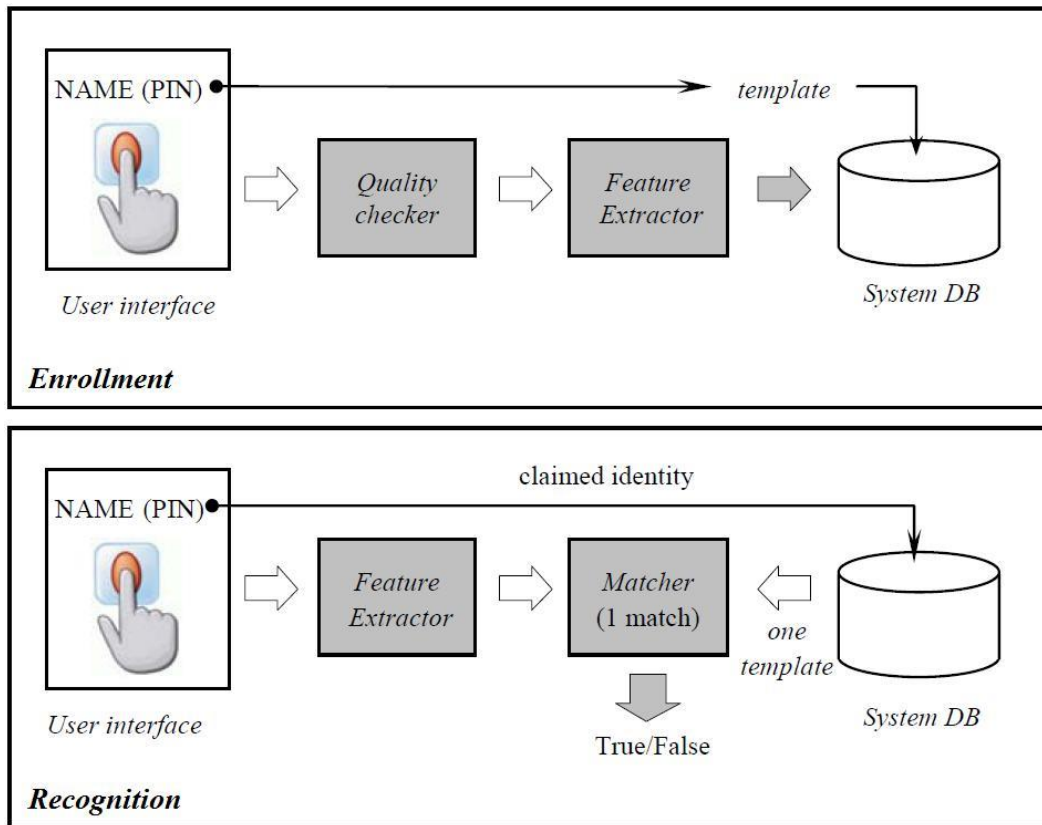
La principal aplicación de la biometría es la autenticación de usuarios bajo el esquema “algo que tú eres” y su amplitud de aplicaciones se basa en lo difícil de alterar. Sin embargo, es una técnica de compleja implementación y de alta tasa de error.

La biometría basa su principio de operación en dos aspectos:

1. Los parámetros biológicos son muy difíciles de suplantar.
2. Cada persona tiene un patrón biológico único, que no se repite ni siquiera en personas gemelas.

¿Cómo opera? Obtiene un patrón digital del parámetro biológico y lo almacena, luego lo compara con la lectura y mide su grado de aproximación. Por ejemplo: huella digital en la cedula de identidad.

Figura 10. Procedimiento de enrolamiento y control en un sistema biométrico



Fuente: <http://biometrics.cse.msu.edu/info/index.html>

Las principales aplicaciones de la biometría son:

- **Reconocimiento facial:** consiste en la comparación de la cara de un usuario contra un patrón preestablecido, por ejemplo: una fotografía, se utiliza cuando se cobra un cheque en el banco.
- **Sistema de autenticación con huella digital:** consiste en comparar el patrón de una huella digital con un archivo previamente establecido. Se utiliza en cajeros automáticos, compra de bonos de isapres o cobro de vale vista.
- **Reconocimiento de voz:** utilizado en sistema de autenticación telefónico.
- **Scan de retina ocular:** a través de un sistema laser se lee la textura de las venas capilares del ojo humano. También se utiliza como control de acceso.
- **Firma en un documento:** basa su principio en que solo el dueño de la firma la puede reproducir.





Los principales aspectos de medición en la biometría son:

- **FAR (False Acceptance Rate):** es la cantidad de identificaciones que dan positivas, sin serlo, por un error en el umbral de aceptación.
- **FRR (False Rejection Rate):** es la cantidad de rechazos que son positivos.
- **FTC (Fail to Capture):** es la falla en la lectura del parámetro.
- **Capacity:** es la cantidad de registros que puede almacenar el sistema.

### 3. POLÍTICAS DE SEGURIDAD

Según la definición de la NIST (2006), es un agregado de directivas, reglas y prácticas que prescribe cómo una organización administra, protege y distribuye información. Es un componente esencial del Gobierno de la seguridad de la información. Sin una política, el gobierno no tiene sustancia ni reglas para hacer cumplir. La política de seguridad de la información debe basarse en una combinación de legislación apropiada y estándares aplicables. Entre sus principales aspectos están:

- Los activos de la compañía considerados valiosos.
- Responsabilidades en algún ítem de seguridad.
- Como resolver alguna situación de conflicto.
- La alineación de la seguridad con los objetivos del negocio.
- Cómo prevenir incidentes de seguridad.
- Responsabilidades legales o normativas.

Los principales ítems de una política de seguridad son:

- Mantener en redes separadas la gestión de los dispositivos y la seguridad.
- Asegurar la eliminación segura de residuos de la empresa.
- Prevenir modificaciones de datos no autorizados.
- Regular la responsabilidad de los usuarios de la compañía y de terceros en el manejo de información.
- Reducir los riesgos por pérdida de información o propiedad intelectual.
- Diferenciar los derechos de accesos de los usuarios.
- Proteger la información confidencial de uso no autorizado.



Según el uso en las organizaciones, se podrían diferenciar los siguientes tipos de políticas:

- **Regulatorias:** permite cumplir algún estándar o normativa a la cual la compañía esté afecta, dependiendo fundamentalmente del tipo de industria.

Ejemplo: una normativa que afecte a la organización puede definir la política de los respaldos de información sensible.

- **Asesoría:** estas permiten dar a conocer a los usuarios su comportamiento ante determinadas situaciones de seguridad, tales como el manejo de información.

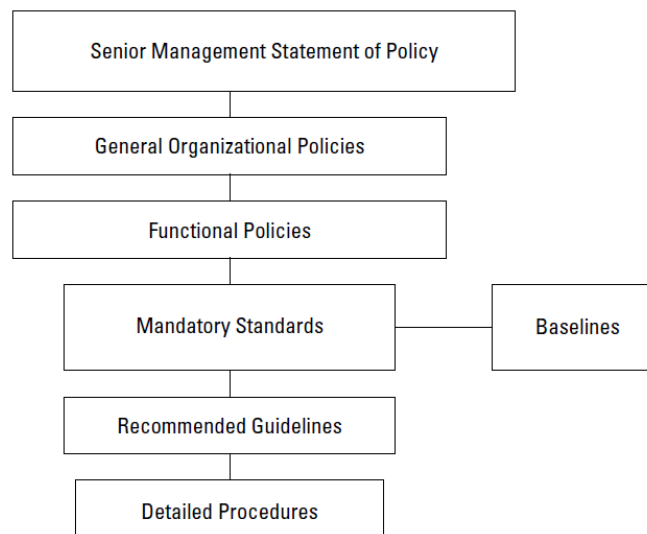
Ejemplo: cada empleado debe activar su protector de pantalla cada vez que se levanta de su escritorio.

- **Informativa:** permite dar a conocer a los usuarios situaciones de seguridad de la compañía con el objeto de capacitarlos y que sean de público conocimiento.

Ejemplo: cualquier indicación de cómo realizar la evacuación de un edificio en caso de emergencia.

Las políticas de seguridad deben seguir un flujo de jerarquía para su aplicación en una organización.

Figura 11. *Jerarquía de las políticas de seguridad*



Fuente: <https://goo.gl/egNkZL>

Según la NIST (2017), en su publicación SP800-12, las políticas de seguridad se pueden clasificar en tres niveles dependiendo de su aplicación:

- **Programa de políticas:** son aquellas que se realizan al más alto nivel de la compañía, afectan a los roles más altos de la empresa y en general no abordan temas específicos.
- **Política específica:** aborda algún tópico general de seguridad de la información, como privacidad o clasificación.
- **Política de sistema:** es aquella que define aspectos técnicos de seguridad de algún sistema, tales como configuración o respaldos.

#### REFLEXIÓN

Una de las principales problemáticas que enfrentan las organizaciones hoy en día es la dificultad que tiene la aplicación de las políticas de seguridad entre los usuarios. Reflexione sobre cuáles pueden ser las causas, de acuerdo con su experiencia, por las que ocurre esta situación.



#### COMENTARIO FINAL

Debido a que en las organizaciones existe gran cantidad de usuarios, con diferentes perfiles y diferentes derechos de acceso, es que se hace necesario aplicar una metodología para gestionar las identidades de los mismos.

Sumado a esto están las múltiples plataformas que utilizan las empresas, por lo que la gestión de identidades y usuarios se torna compleja.

Además, se debe incorporar el ciclo de vida de los usuarios, que abarca desde su ingreso en la compañía hasta su salida o cambio de rol.



## REFERENCIAS

---

Fayerwayer (2018). Parches para Meltdown y Spectre. Recuperado de:

<https://www.fayerwayer.com/2018/01/parches-meltdown-spectre/>

Intypedia [Universidad Politécnica de Madrid](23, 02 2011). Lección 5: Seguridad perimetral.

[Archivo video]. Recuperado de: <https://www.youtube.com/watch?v=sxg1nq17xj4>

NIST (2006). *Seguridad de la información*. Manual: una guía para Gerentes. Recomendaciones del

National Institute of Standards and Technology. Recuperado de:

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>

NIST (2017). *Introduction to Computer Security*. Recomendaciones del National Institute of

Standards and Technology. Recuperado de:

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12.pdf>

PARA REFERENCIAR ESTE DOCUMENTO, CONSIDERE:

IACC (2018). *Seguridad física y lógica*. Ciberseguridad. Unidad 2.



INSTITUTO PROFESIONAL

**iacc**

Autónomo | Reconocido por Mineduc