SEGURIDAD FISICA Y LOGICA

Normativa ISO 27002

- norma internacional ISO/IEC 27002,

- se centra en las buenas prácticas para gestión de la seguridad de la información.

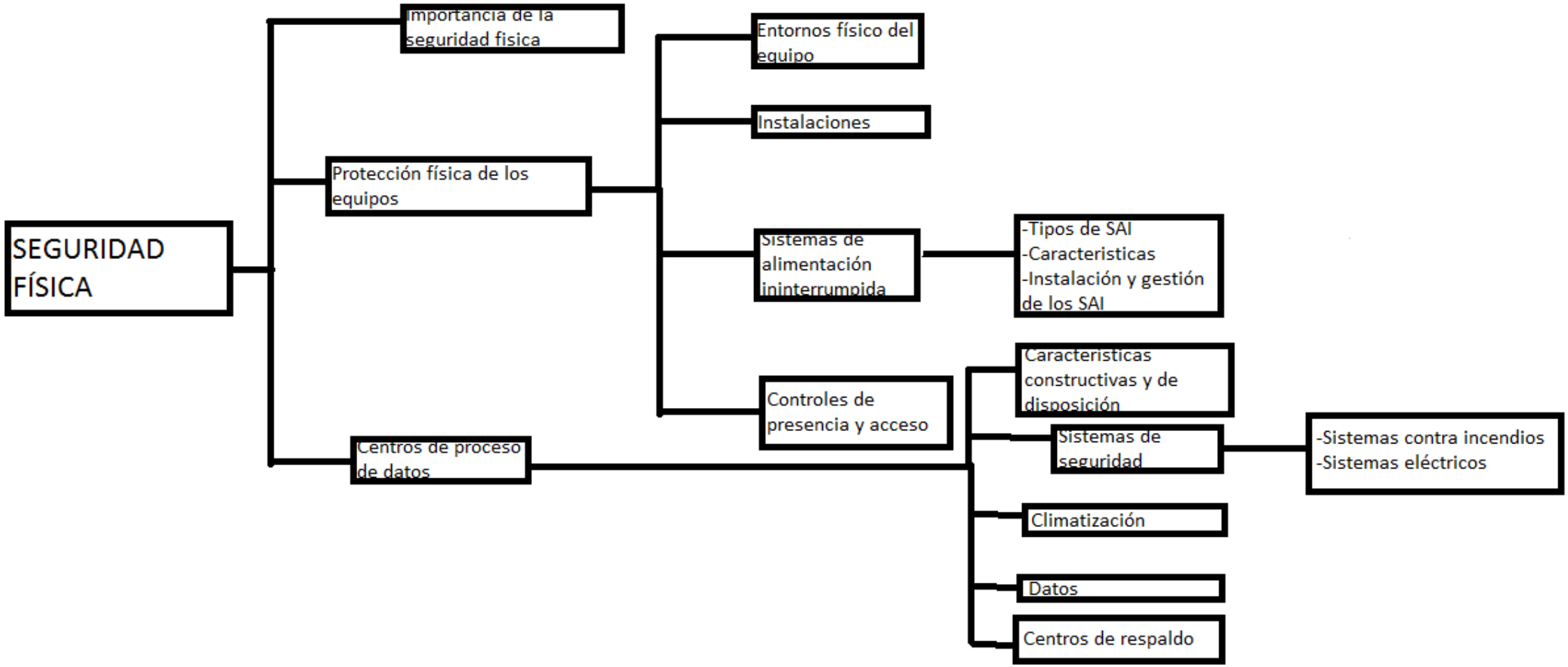
- Es fundamental para la consolidación de un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la continuidad y el mantenimiento de los procesos de seguridad, alineados a los objetivos estratégicos de la organización.

Que es Seguridad Fisica?

- La seguridad física evita y desalienta a los atacantes a ingresar a un edificio instalando cercas, alarmas, cámaras, guardias de seguridad y perros, control de acceso electrónico, detección de intrusos y controles de acceso de administración.


CONTROL DE ACCESO
DETECCIÓN DE INTRUSOS
SEGURIDAD DE LA INFORMACIÓN
CENTRO DE BASES DE DATOS
GESTIÓN DE VISITANTES Y RECONOCIMIENTO DE IDENTIDAD
GESTIÓN DE ACTIVOS
COMUNICACIONES DE EMERGENCIAS
SISTEMAS UNIFICADOS
SENSORES Y ALARMAS
VIDEO VIGILANCIA
SEGURIDAD FÍSICA

Amenazas	Mecanismos de defensa
Incendios	◆ El mobiliario de los centros de cálculo debe ser ignífugo. ◆ Evitar la localización del centro de procesamiento de datos cerca de zonas donde se manejen o almacenen sustancias inflamables o explosivos. ◆ Deben existir sistemas antiincendios, detectores de humo, rociadores de gas, extintores… para sofocar el incendio en el menor tiempo posible y así evitar que se propague ocasionando numerosas pérdidas materiales.
Inundaciones	◆ Evitar la ubicación de los centros de cálculo en las plantas bajas de los edificios para protegerse de la entrada de aguas superficiales. ◆ Impermeabilizar las paredes y techos del Centro de Cálculo. Sellar las puertas para evitar la entrada de agua proveniente de las plantas superiores.
Robos	◆ Proteger los centros de cálculo mediante puertas con medidas biométricas, cámaras de seguridad, vigilantes jurados…, con todas estas medidas pretendemos evitar la entrada de personal no autorizado.
Señales Electromagnéticas	◆ Evitar la ubicación de los centros de cálculo próximos a lugares con gran radiación de señales electromagnéticas, pues pueden interferir en el correcto funcionamiento de los equipos informáticos del cableado de red. ◆ En caso de no poder evitar la ubicación en zonas con grandes emisiones de este tipo de señales deberemos proteger el centro frente de dichas emisiones mediante el uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.
Apagones	◆ Para evitar los apagones colocaremos Sistemas de Alimentación Ininterrumpida (SAI), que proporcionan corriente eléctrica durante un periodo de tiempo suficiente.
Sobrecargas Eléctricas	◆ Además de proporcionar alimentación, los SAI profesionales incorporan filtros para evitar picos de tensión, es decir, estabilizan la señal eléctrica.
Desastres Naturales	◆ Estando en continuo contacto con el Instituto Geográfico Nacional y de Meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos en España.


SEGURIDAD FÍSICA
Importancia de la seguridad fisica
Protección física de los equipos
Centros de proceso de datos
Entornos físico del equipo
Instalaciones
Sistemas de alimentación ininterrumpida
Controles de presencia y acceso
-Tipos de SAI
-Caracteristicas
-Instalación y gestión de los SAI
Caracteristicas constructivas y de disposición
Sistemas de seguridad
Climatización
Datos
Centros de respaldo
-Sistemas contra incendios
-Sistemas eléctricos

Medidas en CPD

- Seguridad ambiental
  - Medidas contra fallos eléctricos
  - Equipos de control de temperatura y humedad
  - Medidas contra incendios
  - Detectores de agua
  - Planes de evacuación
  - Prohibir entrar comida y bebida

Control de CPD

- Temperatura entre 21 grados +- 3
- Humedad 50% evitando riesgo de condensación y estática

Que es Seguridad Logica?

- La seguridad lógica protege el software informático al desalentar el exceso de usuarios mediante la implementación de identificaciones de usuario, contraseñas, autenticación, biometría y tarjetas inteligentes.

- La Seguridad Lógica consiste en la «*aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo permitan acceder a ellos a las personas autorizadas para hacerlo*«.
- Los objetivos que se plantean serán:
- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no les correspondan.

Medidas a aplicar para mejorar la seguridad lógica

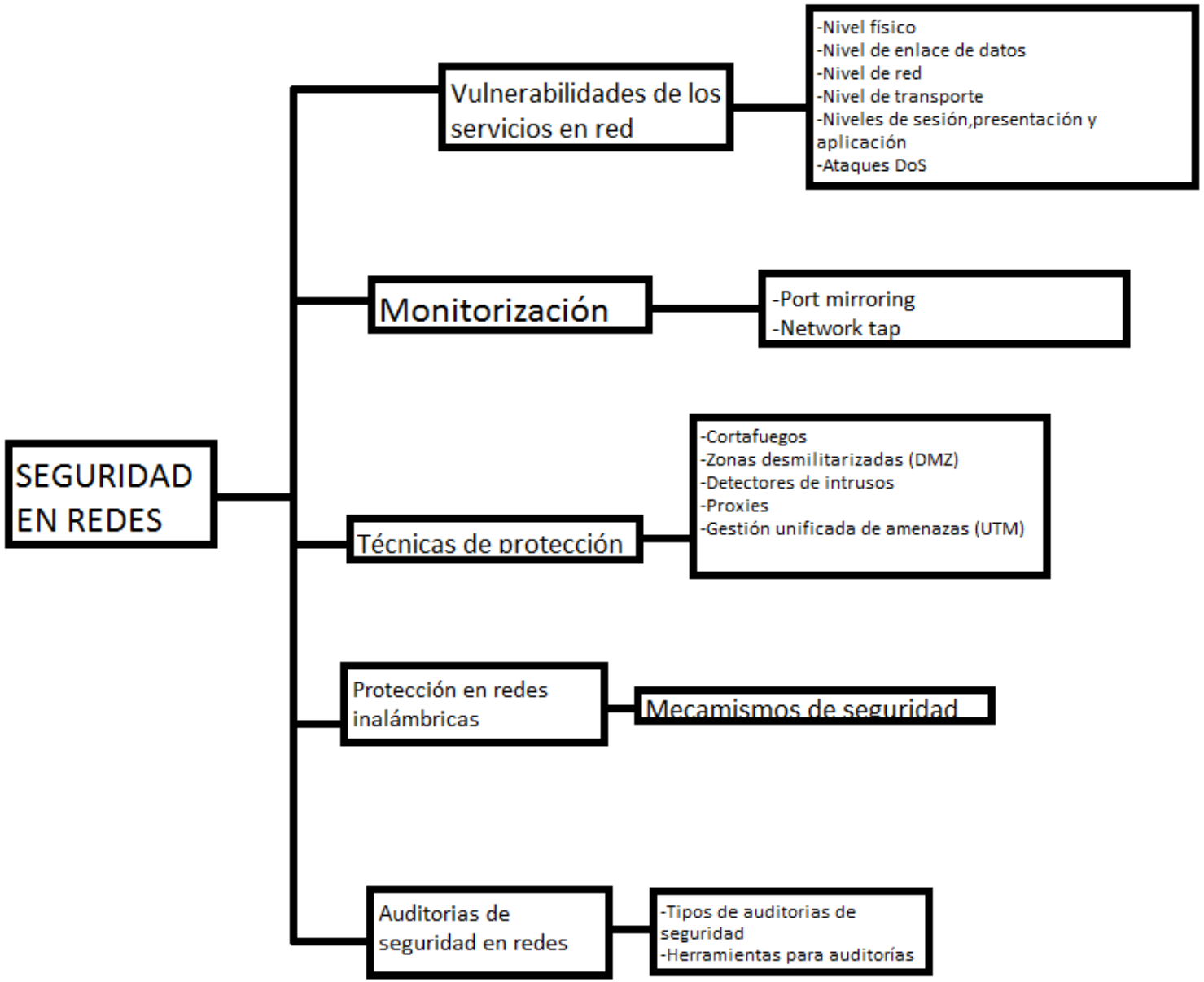
- Por ejemplo, las contraseñas y códigos de acceso que usa para acceder a tu ordenador, tu teléfono y tus sitios web y servicios en línea favoritos son todas instancias de control de acceso lógico.
- En este proceso, la combinación correcta de nombre de usuario y contraseña verifica el permiso para acceder a ciertas funciones dentro de una organización como usuario, empleado o cliente. Este tipo de autenticación es solo uno de un número creciente de controles de acceso lógico.
- La autenticación es una de las medidas de seguridad lógica más populares en el espacio de ciberseguridad. Sin embargo, las estrategias de autenticación están avanzando cada año, y la autenticación de contraseña tradicional ya no es suficiente contra el rango de amenazas que enfrentan las empresas.

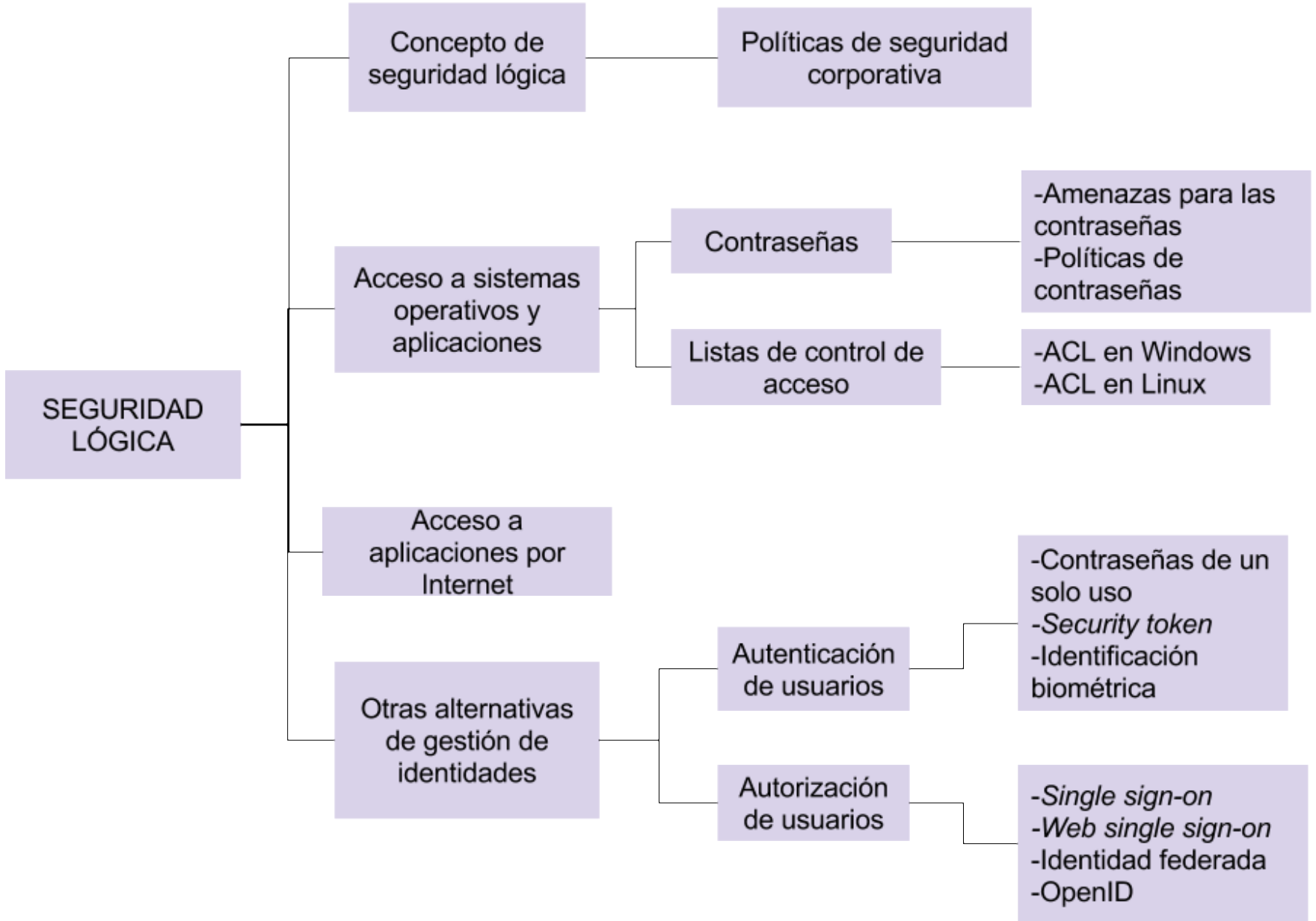
Medidas a aplicar para mejorar la seguridad lógica

- La autenticación de tokens es una de estas medidas. En este modelo, los tokens de seguridad proporcionan a los usuarios un número que cambia en una línea de tiempo determinada, generalmente cada minuto. Como parte de un proceso de inicio de sesión, los sistemas empresariales solicitarán a los usuarios el token y lo compararán con los mecanismos internos para garantizar que el token sea correcto.
- La autenticación de dos factores (2FA) es otra área emergente de seguridad lógica. Además de un nombre de usuario y contraseña, los usuarios pueden tener que proporcionar respuestas a preguntas de seguridad o confirmar un PIN enviado a un dispositivo o aplicación por separado.

Medidas a aplicar para mejorar la seguridad lógica

- Además de los tipos de autenticación, que incluso pueden incluir medidas biométricas, hay otras medidas de seguridad lógicas disponibles.
- Por ejemplo, la segmentación de usuarios permite a los administradores del sistema controlar las áreas de la red de la organización a las que pueden acceder los usuarios individuales. Esto garantiza que, en caso de que la cuenta de un usuario se vea comprometida de alguna manera, el atacante no podrá causar estragos en toda la red de la organización.


SEGURIDAD EN REDES
Vulnerabilidades de los servicios en red
-Nivel físico
-Nivel de enlace de datos
-Nivel de red
-Nivel de transporte
-Niveles de sesión,presentación y aplicación
-Ataques DoS
Monitorización
-Port mirroring
-Network tap
Técnicas de protección
-Cortafuegos
-Zonas desmilitarizadas (DMZ)
-Detectores de intrusos
-Proxies
-Gestión unificada de amenazas (UTM)
Protección en redes inalámbricas
Mecamismos de seguridad
Auditorias de seguridad en redes
-Tipos de auditorias de seguridad
-Herramientas para auditorías


SEGURIDAD LÓGICA
Concepto de seguridad lógica
Políticas de seguridad corporativa
Acceso a sistemas operativos y aplicaciones
Contraseñas
-Amenazas para las contraseñas
-Políticas de contraseñas
Listas de control de acceso
-ACL en Windows
-ACL en Linux
Acceso a aplicaciones por Internet
Otras alternativas de gestión de identidades
Autenticación de usuarios
-Contraseñas de un solo uso
-Security token
-Identificación biométrica
Autorización de usuarios
-Single sign-on
-Web single sign-on
-Identidad federada
-OpenID

- Active directory
- Kerberos
- Open LDAP

Active Directory

- Active Directory (AD) es una base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo.
- La base de datos (o el directorio) contiene información crítica sobre su entorno, incluidos los usuarios y las computadoras que hay y quién puede hacer qué. Por ejemplo, la base de datos puede contener una lista de 100 cuentas de usuario con detalles como el puesto de trabajo, el número de teléfono y la contraseña de cada persona. También registrará sus permisos.
- Los servicios controlan gran parte de la actividad que se desarrolla en su entorno de TI. En particular, se aseguran de que cada persona sea quien dice ser (autenticación), generalmente al verificar el ID de usuario y la contraseña que ingresa, y le permite acceder solo a los datos que tiene permitido usar (autorización).

Kerberos

- Kerberos es un protocolo de autenticación, pero no de autorización. Esto quiere decir que el protocolo se encarga de identificar a cada usuario, a través de una contraseña solo conocida por este, pero no determina a qué recursos o servicios puede acceder o no dicho usuario.
- Kerberos es ampliamente utilizado en Active Directory. En esta plataforma Kerberos da información de los privilegios de cada usuario autenticado, pero queda a cargo de los servicios el verificar que dichos privilegios son suficientes para acceder a sus recursos.

LDAP

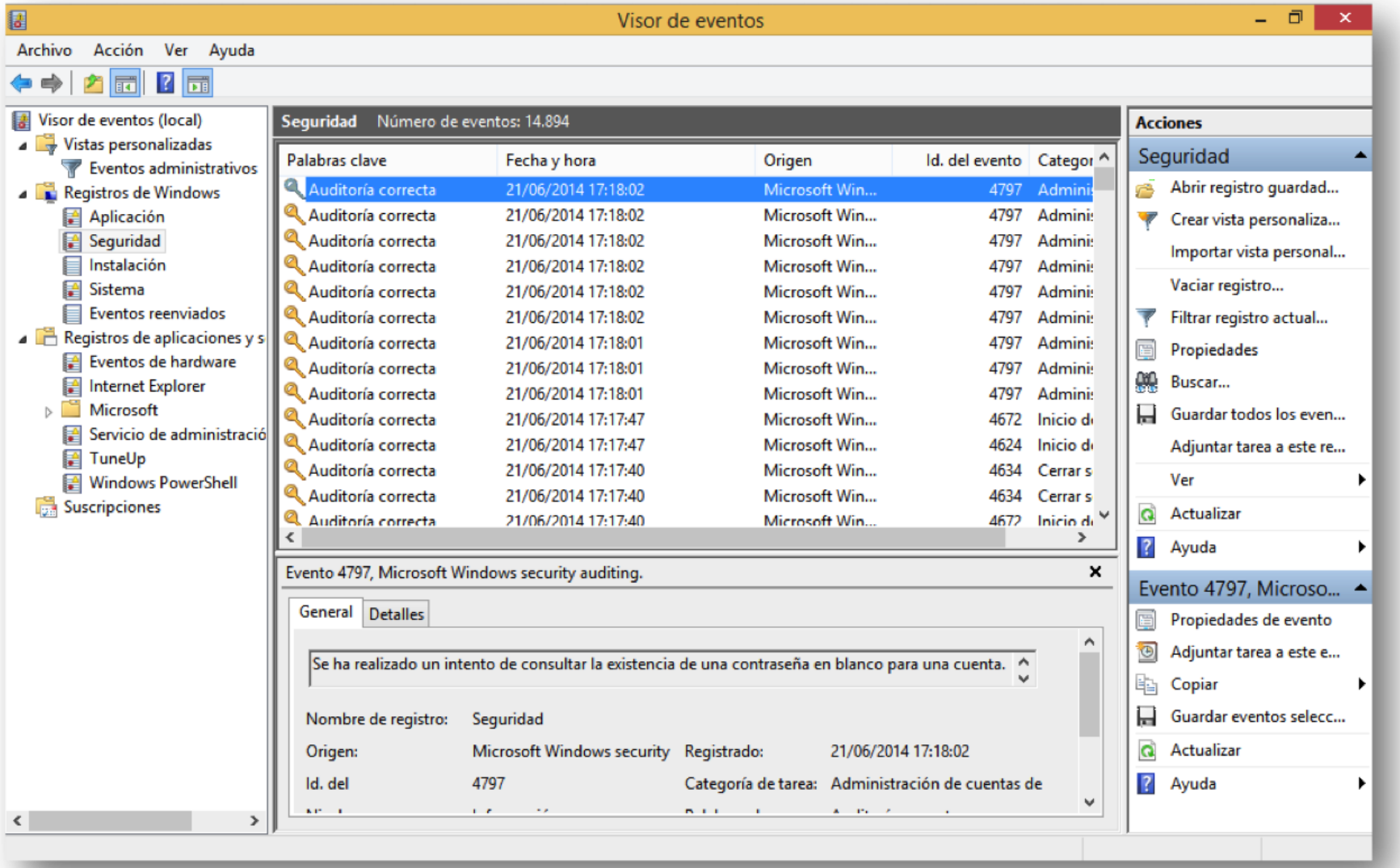
- Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios) y es un mecanismo importante en el inicio de sesión de los ordenadores en red, sobre todo dentro de las empresas.

Listas de Control de Acceso

- Las clistas de control de acceso para un fichero o directorio, definen que usuarios autentificados pueden acceder a un fichero, y que tareas pueden realizar.

- Windows: cacls
- Linux: chmod

Registros windows




Panel de control
Herramientas administrativas
Impresoras y faxes
Ayuda y soporte técnico
Buscar
Ejecutar...
Seguridad de Windows
Administrador de equilibrio de carga de red
Administrador de Servicios de Terminal Server
Administre su servidor
Asistente para configurar su servidor
Asistentes de Microsoft .NET Framework 1.1
Configuración de Microsoft .NET Framework 1.1
Configuración de Servicios del Terminal Server
DHCP
Directiva de seguridad local
Enrutamiento y acceso remoto
Entidad emisora de certificados
Escritorios remotos
Licencias de Terminal Server
Orígenes de datos (ODBC)

Diferencias

- La diferencia entre la seguridad lógica y la seguridad física es que la seguridad lógica protege el acceso a los sistemas informáticos y la seguridad física protege el sitio y todo lo que se encuentra dentro del sitio.
- El término Seguridad lógica se utiliza coloquialmente para referirse a medidas electrónicas como los permisos dentro del sistema operativo o las reglas de acceso en las capas de la red, como el firewall, enrutadores y conmutadores.
- La seguridad física se usa tradicionalmente para describir puertas de entrada controladas, videovigilancia y otras medidas metafísicas.

- Asegurar que se estén utilizando los datos, archivos y programas correctos por el procedimiento correcto.
- Que la información transmitida sea recibida por el destinatario al que ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información