## IFCT0109. SEGURIDAD INFORMÁTICA

# MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

# UD06

## SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE LOS SISTEMAS



DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

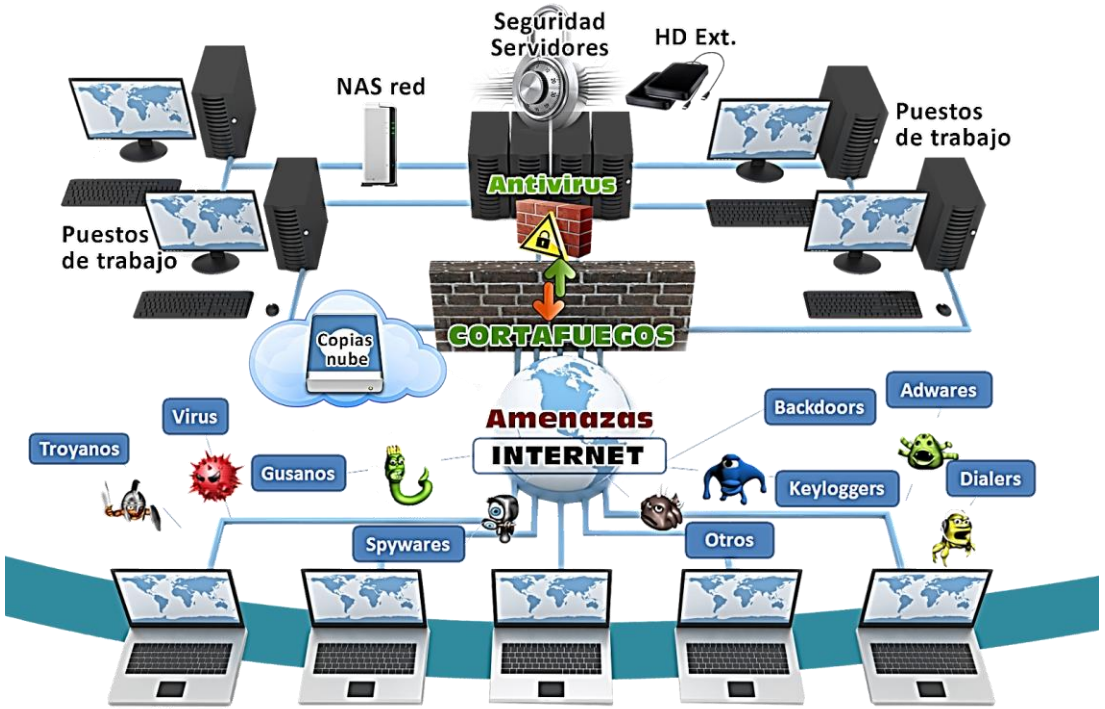
# CONTENIDOS

## 1. INTRODUCCIÓN

2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

# 1. INTRODUCCIÓN

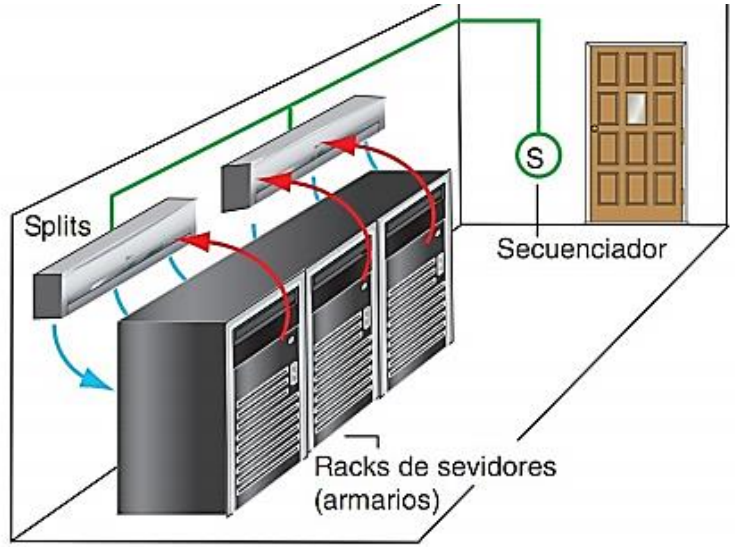
LA SEGURIDAD DE LA INFORMACIÓN (**SI**) DEBE ABORDARSE DESDE UNA PERSPECTIVA INTEGRAL, QUE ABARQUE **LA SEGURIDAD FÍSICA (SF)** Y LA **SEGURIDAD LÓGICA (SL)**.



# 1. INTRODUCCIÓN

LA **SEGURIDAD FÍSICA (SF) SE OCUPA DEL CONJUNTO DE BARRERAS FÍSICAS**, PROCEDIMIENTOS, Y MECANISMOS DE CONTROL, PARA PROTEGER LOS ACTIVOS DE LAS AMENAZAS FÍSICAS, EN EL ENTORNO DE LA EMPRESA Y SUS SISTEMAS DE INFORMACIÓN.

*LAS AMENAZAS FÍSICAS SE ORIGINAN Y PROCEDEN DEL HOMBRE (INVOLUNTARIAMENTE), O DE LA NATURALEZA*.



# 1. INTRODUCCIÓN

LA **SEGURIDAD LÓGICA (SL) SE OCUPA DEL CONJUNTO DE BARRERAS LÓGICAS**, PROCEDIMIENTOS, Y MECANISMOS DE CONTROL, PARA PROTEGER LOS ACTIVOS RESGUARDADOS E ÍNTEGROS, PERMITIENDO EL ACCESO LÓGICO SOLO A LOS AGENTES AUTORIZADOS PARA ELLO.

# 1. INTRODUCCIÓN

**SF** Y **SL** SON UNA DIVISIÓN CLÁSICA DE LA **SI**, Y DEBEN IMPLANTARSE DE FORMA EQUILIBRADA.

**AMBAS SON NECESARIAS Y FORMAN UN TODO** (**SI**), ES DECIR, LA AUSENCIA DE UNA HACE INÚTIL LA EXISTENCIA DE LA OTRA.

ESTE CAPÍTULO SE CENTRA EN ASPECTOS PRÁCTICOS DE IMPLEMENTACIÓN DE **SF** Y **SL**, INCLUYENDO LAS ÁREAS DE ESTUDIO Y CONTRAMEDIDAS MÁS USUALES.

TOMAREMOS COMO REFERENCIA LO QUE LA NORMA **ISO 27002** DICTA, EN LOS OBJETIVOS DE CONTROL DE SU **CAPÍTULO 9**, DEDICADO A LA **SEGURIDAD FÍSICA Y AMBIENTAL**, Y EN LOS OBJETIVOS DE CONTROL DE SU **CAPÍTULO 11**, DEDICADO AL **CONTROL DE ACCESO**.

# CONTENIDOS

1. INTRODUCCIÓN
2. **DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA**
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

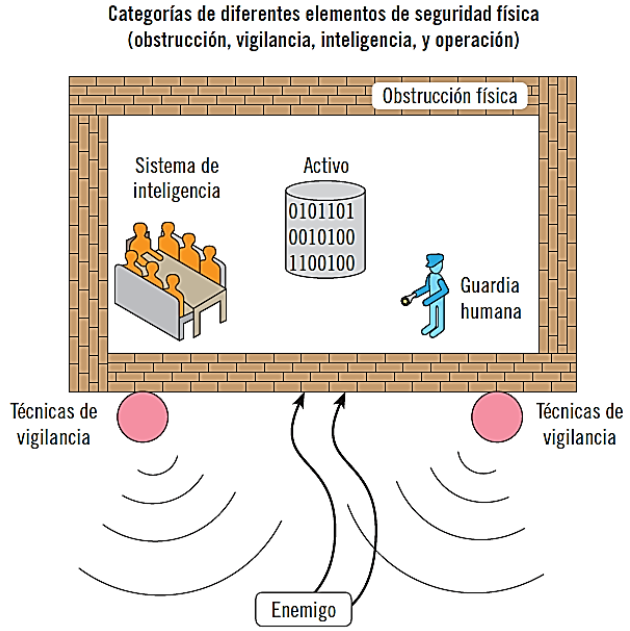
**LOS FUNDAMENTOS DE LA SI PROCEDEN DE LAS IDEAS ESENCIALES DE LA SEGURIDAD**, QUE A SU VEZ NACEN DE *CONCEPTOS DE ORIGEN MILITAR* EN *SITUACIONES DE BATALLA Y DE GUERRA*.

A CONTINUACIÓN, SE INTRODUCEN ALGUNOS CONCEPTOS GENERALES DE SEGURIDAD FÍSICA, PARA POSTERIORMENTE CONCRETAR LAS MEDIDAS EN **SF** QUE DA LA NORMA **ISO 27002** EN EL CAMPO DE LA **SI**.

# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

LOS CONCEPTOS GENERALES DE **SF** SE DESARROLLAN EN UN **ESCENARIO DE GUERRA, CONTRA UN ENEMIGO QUE PRETENDE VULNERAR LAS MEDIDAS DE CONTROL Y CONTENCIÓN** QUE TIENE EL OBJETIVO ATACADO, PARA APODERARSE DE ESTE.



# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

ESTA PERSPECTIVA SE MATERIALIZA EN LOS SIGUIENTES **CUATRO** ELEMENTOS, O **CATEGORÍAS** HABITUALES **DE LA SEGURIDAD FÍSICA**:

- **LAS OBSTRUCCIONES FÍSICAS**
- **LAS TÉCNICAS DE VIGILANCIA**
- **LOS SISTEMAS DE INTELIGENCIA**
- **LOS GUARDIAS O PERSONAL DE SEGURIDAD**

# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

**LAS OBSTRUCCIONES FÍSICAS**, QUE PLANTEAN UN RETO A QUIEN PRETENDA TRASPASARLAS.

**LAS TÉCNICAS DE VIGILANCIA**, QUE ALERTAN DE CUALQUIER MOVIMIENTO PERCIBIDO EN EL PERÍMETRO DE ACCESO.

**LOS SISTEMAS DE INTELIGENCIA**, QUE ANALIZAN LA INFORMACIÓN DE VIGILANCIA, E INCLUSO INDAGAN MÁS ALLÁ DE SUS LÍMITES, PARA OBTENER VENTAJAS TÁCTICAS Y OPERATIVAS ANTE AMENAZAS.

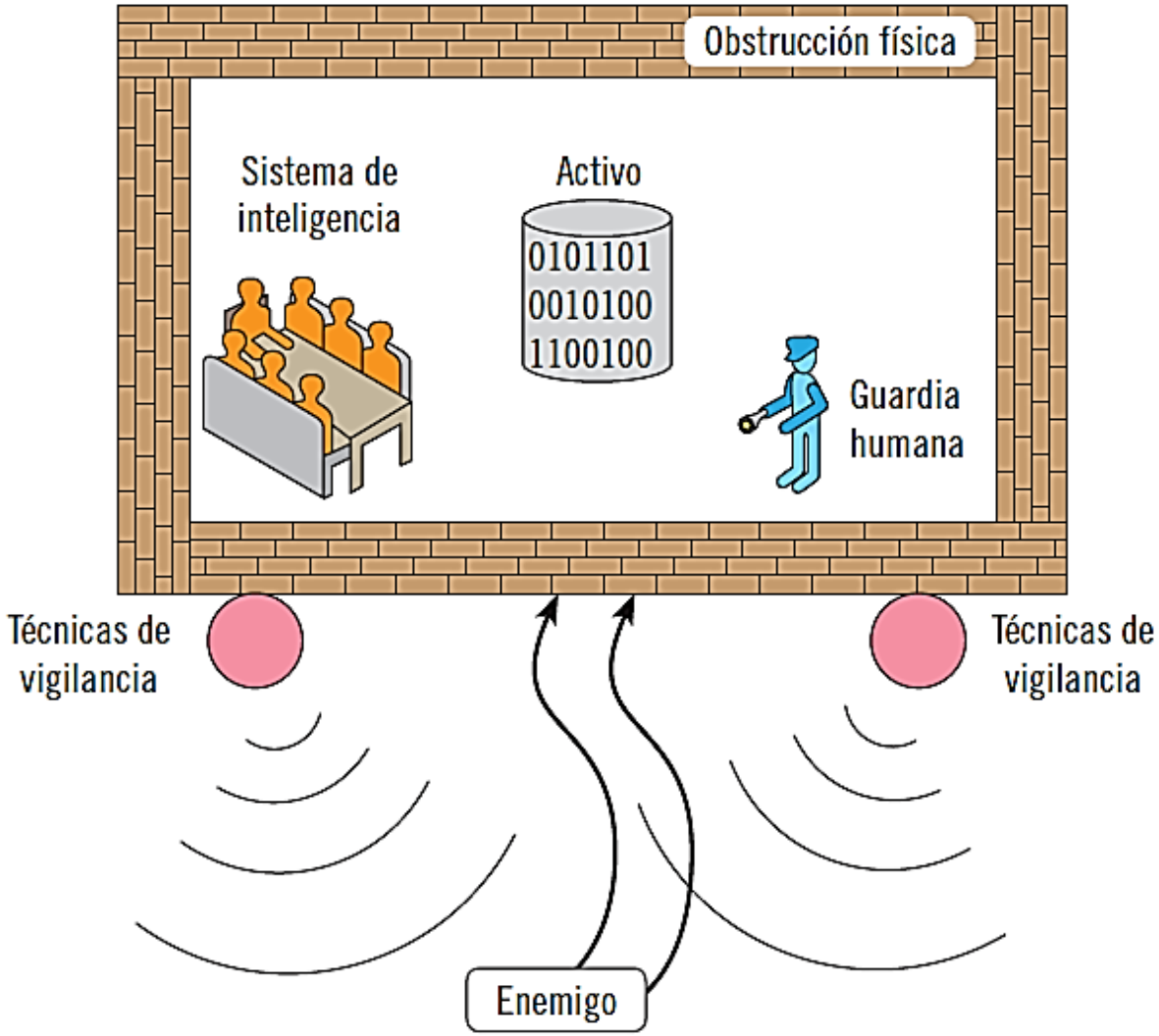
**LOS GUARDIAS O PERSONAL DE SEGURIDAD**, QUE APORTAN LA INTELIGENCIA HUMANA, Y EFECTIVIDAD OPERACIONAL ANTE UNA AMENAZA, ACTUANDO Y DECIDIENDO FRENTE A UNA ALARMA.

# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

### CATEGORÍAS DE DIFERENTES ELEMENTOS DE SEGURIDAD FÍSICA

# OBSTRUCCIÓN, VIGILANCIA, INTELIGENCIA, Y OPERACIÓN



# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

EL ELEMENTO CENTRAL DE LA SEGURIDAD ES **EL ACTIVO**, QUE DEBE ESTAR SIEMPRE **FÍSICAMENTE LOCALIZADO**

LOS **ACTIVOS DE INFORMACIÓN**, POR NORMA GENERAL, TENDRÁN UNA ARQUITECTURA **CLIENTE-SERVIDOR**, DONDE INTERVIENEN LOS SIGUIENTES ELEMENTOS Y UBICACIONES:

- **UN ORDENADOR CENTRAL O SERVIDOR**
- **UN CLIENTE**
- **UNA RED DE COMUNICACIONES**

# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

**UN ORDENADOR CENTRAL O SERVIDOR**

QUE **ALOJA LOS DATOS** (ACTIVOS) Y TAMBIÉN **LAS APLICACIONES**. ESTARÁ LOCALIZADO BIEN **EN LAS PROPIAS INSTALACIONES DE LA EMPRESA, O BIEN FUERA DE ELLA**.

LAS **TÉCNICAS DE VIRTUALIZACIÓN** CONFIEREN MOVILIDAD A LOS SERVIDORES, QUE PASAN A SER DATOS EJECUTADOS POR UNO O VARIOS SERVIDORES FÍSICOS; POR LO TANTO, **LA UBICACIÓN DE UN SERVIDOR VIRTUAL, ES LA DE LOS SERVIDORES FÍSICOS QUE PUEDEN EJECUTARLO**.

EN CUALQUIER CASO, **UN SERVIDOR**, FÍSICO O VIRTUAL, SIEMPRE **DEBE ESTAR LOCALIZADO EN UN CENTRO DE PROCESO DE DATOS** (O **CPD**), QUE SERÁ UN RECINTO DEDICADO ESPECÍFICAMENTE A ESTE FIN, Y DONDE HABITUALMENTE SE HOSPEDAN O ALBERGAN MÚLTIPLES SERVIDORES.

# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

**UN CLIENTE**

**SE CONECTA AL SERVIDOR PARA ACCEDER A LOS DATOS DE ÉSTE, Y QUE TAMBIÉN PUEDE ALBERGAR DATOS Y APLICACIONES.**

EL CLIENTE **PUEDE ESTAR LOCALIZADO EN LA EMPRESA O FUERA DE ELLA**.

CADA VEZ MÁS, EXISTEN CLIENTES MÓVILES, COMPLETAMENTE DESLOCALIZADOS, COMO SON LOS ORDENADORES PORTÁTILES, O LOS TELÉFONOS MÓVILES.

# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

### UNA RED DE COMUNICACIONES

**CONECTA AL CLIENTE Y AL SERVIDOR**, Y POR LA QUE TRANSITAN LOS ACTIVOS O DATOS. LA RED PARTE DE LA UBICACIÓN DEL SERVIDOR, Y TERMINA EN LA UBICACIÓN DEL CLIENTE.

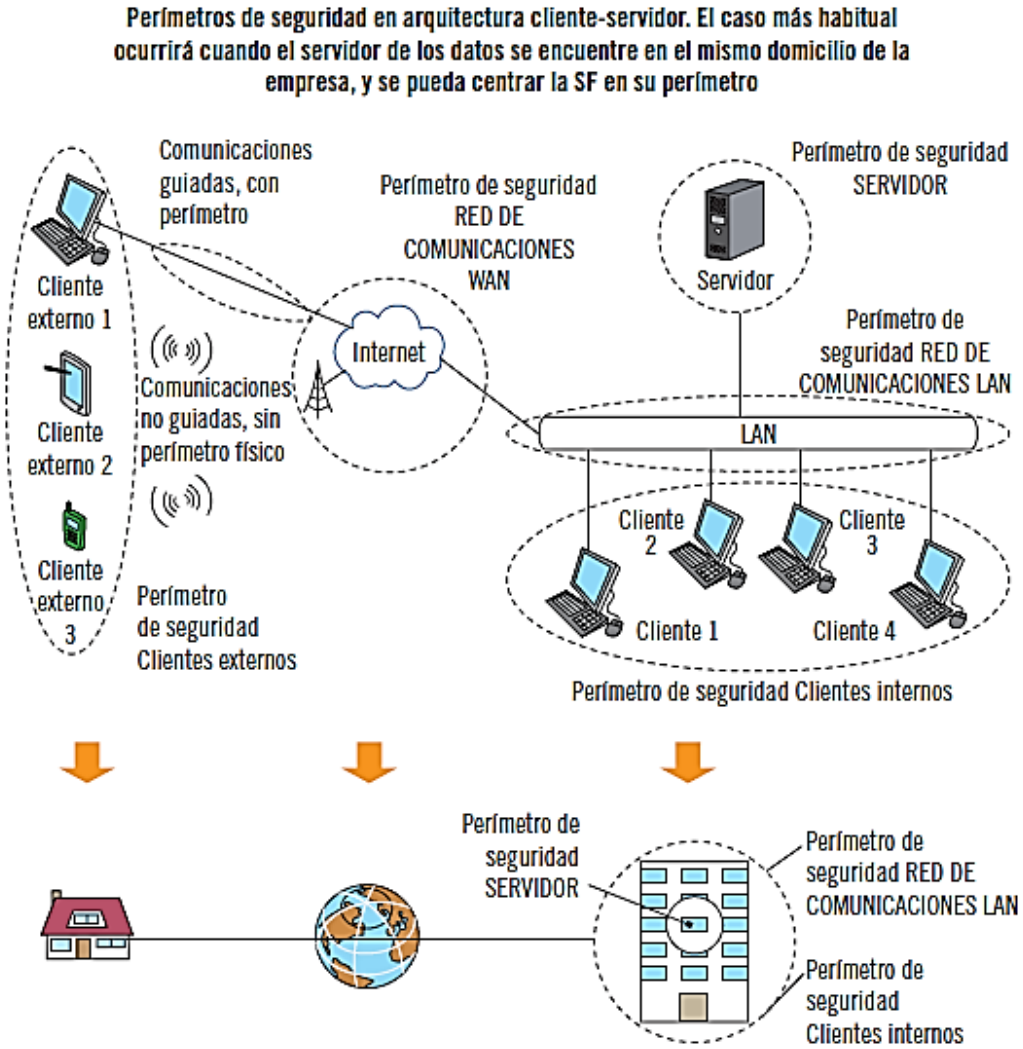
**SE ENCONTRARÁ** HABITUALMENTE **UN TRAMO PRIVADO** CONFINADO A LAS INSTALACIONES DE LA EMPRESA Y DE SU PROPIEDAD, QUE CONSTITUYE UNA RED DE ÁREA LOCAL (**LAN**), **Y,** EN SEGUNDO LUGAR, **UN TRAMO PÚBLICO**, QUE LA RED DE ÁREA EXTENSA (**WAN**), QUE RESULTA ACCESIBLE DESDE LAS REDES DE COMUNICACIONES PÚBLICAS DE ACCESO A ABONADOS TELEFÓNICOS, Y LAS REDES DE TELEFONÍA MÓVIL.

# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

EL **PERÍMETRO FÍSICO A PROTEGER** SERÍA EL ENTORNO FÍSICO DE TODOS ESTOS ELEMENTOS, INCLUIDAS LAS REDES O CAMINOS POR DONDE TRANSITA EL ACTIVO.

RESULTA **DESPROPORCIONADO** EN EL CASO DE LAS **REDES WAN** Y EL **TRÁNSITO POR INTERNET**; TAMBIÉN RESULTA DIFÍCIL A **LOS CLIENTES EXTERNOS O EN MOVILIDAD**.



# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

**SE SUELE PRIORIZAR EL PERÍMETRO DEL SERVIDOR**, ALOJADO EN EL **CPD**.

POSTERIORMENTE, EL **PERÍMETRO DE LOS CLIENTES INTERNOS**, Y DE **LA RED DE COMUNICACIONES INTERNA** A LA EMPRESA O LAN.

**EL CPD** DONDE SE ALOJA EL SERVIDOR **TAMBIÉN ALOJARÁ LOS EQUIPOS MÁS IMPORTANTES DE LA RED DE COMUNICACIONES LAN**.

LA SIGUIENTE ES UNA **LISTA DE LAS INSTALACIONES** QUE DEBERÍAN CONSIDERARSE INCLUIR EN EL PERÍMETRO DE **SF**, SIEMPRE BAJO UN CRITERIO DE PROPORCIONALIDAD.

# 2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA

## CONCEPTOS GENERALES DE SEGURIDAD FÍSICA

- LA SALA DE COMPUTADORAS O CPD
- LOS ARMARIOS DE COMUNICACIONES QUE PUEDA HABER FUERA DEL CPD
- LOS EQUIPOS DE TELECOMUNICACIONES, INCLUYENDO LAS CONEXIONES DE RED EXTERNAS
- ÉL ÁREA DE DESARROLLO O DE PROGRAMACIÓN
- LAS CONSOLAS Y TERMINALES DE LOS OPERADORES
- LAS BIBLIOTECAS DE CINTAS, DISCOS, CD, SOPORTES USB, Y OTROS MEDIOS DE ALMACENAMIENTO, INCLUIDAS LAS COPIAS DE SEGURIDAD, LAS SALAS DONDE SE GUARDEN ESTOS SOPORTES O SUS SUMINISTROS, Y LOS EMPLAZAMIENTOS EXTERNOS, SI LAS COPIAS DE RESPALDO SE SACAN DE LA EMPRESA
- LAS ESTACIONES DE TRABAJO Y COMPUTADORES PERSONALES
- LAS FUENTES DE ENERGÍA
- LOS SITIOS DONDE SE GUARDAN TEMPORALMENTE LOS DESECHOS
- LOS TELÉFONOS Y LÍNEAS TELEFÓNICAS DEDICADAS
- LOS EQUIPOS PORTÁTILES
- LAS IMPRESORAS LOCALES
- LA RED DE ÁREA LOCAL, EN TODAS SUS TOMAS Y RECORRIDOS
- LA DOCUMENTACIÓN DEL SISTEMA Y DE LA INFRAESTRUCTURA

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. **SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS**
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

EL **CPD** ES LA **PRIMERA ÁREA A PROTEGER**, PORQUE **ALBERGA EL SERVIDOR, Y LOS ELEMENTOS MÁS CRÍTICOS DE COMUNICACIONES**.

LA PROTECCIÓN SE DEBERÍA AMPLIAR A TODA LA EMPRESA, QUE ALBERGA EL **RESTO DE LA RED DE COMUNICACIONES** Y LOS **CLIENTES INTERNOS**, ADEMÁS DE OTRAS INSTALACIONES.

**ES PRIORITARIA LA SF DEL CPD**, PORQUE ES LA UBICACIÓN CON **MAYOR DENSIDAD DE ACTIVOS** O **VALOR EN INFORMACIÓN**.

ADEMÁS, **ES MÁS FÁCIL DE PROTEGER** QUE EL INMUEBLE AL COMPLETO.

A CONTINUACIÓN, SE PRESENTARÁN **LOS RIESGOS Y LOS CONTROLES DE ACCESO FÍSICO** PARA REDUCIRLOS.

## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

### RIESGOS DEL ACCESO FÍSICO

CON ACCESO FÍSICO AL SERVIDOR, **SE PUEDEN MATERIALIZAR INCIDENTES DE SEGURIDAD DE LA MÁXIMA SEVERIDAD**. EL RIESGO EXISTE SIEMPRE QUE HAYA ACCESO. **LOS ACTORES DE LA AMENAZA SERÁN**:

- EMPLEADOS O PERSONAL SUBCONTRATADO POR LA EMPRESA, AUTORIZADOS O NO
- PERSONAL TÉCNICO DE PROVEEDORES
- VISITAS
- PERSONAL ANTIGUO, EMPLEADO O SUBCONTRATADO POR LA EMPRESA
- LADRONES U OTROS DELINCUENTES, EN BENEFICIO PROPIO, O CONTRATADOS POR LA COMPETENCIA

## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

### RIESGOS DEL ACCESO FÍSICO. TIPOS DE INCIDENTES POR ACCESO FÍSICO

CON **CARÁCTER INVOLUNTARIO O NO INTENCIONADO**, PUEDEN SURGIR ACCIDENTES.

CON **CARÁCTER VOLUNTARIO O INTENCIONADO**, *LA SITUACIÓN ES INCLUSO PEOR*, PORQUE EL INCIDENTE INTENCIONADO ACARREA FÁCILMENTE LA ABSOLUTA PÉRDIDA DE SEGURIDAD DE LA INFORMACIÓN, SIENDO SUSTRAÍDA, CORROMPIDA, O BORRADA POR COMPLETO.

UN INCIDENTE DIRIGIDO PUEDE SUPONER GRAVES PERJUICIOS PARA LA EMPRESA, COMO PROBLEMAS LEGALES, PÉRDIDAS ECONÓMICAS, DE REPUTACIÓN, Y COMPETITIVIDAD.

## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

### RIESGOS DEL ACCESO FÍSICO. TIPOS DE INCIDENTES POR ACCESO FÍSICO

LOS **PRINCIPALES RIESGOS** SON:

- DESTRUCCIÓN ABSOLUTA DE LA INFORMACIÓN Y LOS EQUIPOS
- DAÑO A LOS EQUIPOS
- SUSTRACCIÓN DE LOS EQUIPOS
- ACCESO Y PUBLICACIÓN DE INFORMACIÓN CONFIDENCIAL
- MODIFICACIÓN DEL SISTEMA O DE LA INFORMACIÓN PRIVADA QUE GUARDEN
- ACCESO NO AUTORIZADO AL SISTEMA Y SU CONFIGURACIÓN, REDUCIENDO SU DISPONIBILIDAD
- USO FRAUDULENTO DEL SISTEMA O DE LA INFORMACIÓN PRIVADA
- SECUESTRO O CHANTAJE
- EJECUCIÓN DE APLICACIONES MALICIOSAS PARA ESPIONAJE Y CONTROL REMOTO DE LOS SISTEMAS

## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

### CONTROLES DE ACCESO FÍSICO

LOS SIGUIENTES **CONTROLES**, DEBEN CONSIDERARSE EN MAYOR O MENOR PROFUNDIDAD, CON PROPORCIONALIDAD A LOS RIESGOS DE SI QUE AFRONTE LA EMPRESA. SON APLICABLES, TANTO AL CPD COMO A TODA LA EMPRESA.

- **ÁREA DE RECEPCIÓN DE PERSONAS**
- **REGISTRO DE ENTRADAS Y SALIDAS**
- **TRATAMIENTO DE PERSONAL EXTERNO**
- **GUARDIAS**
- **ENTRADAS DE DOBLE PUERTA**
- **PUERTAS DE CONTROL ELECTRÓNICO**
- **CÁMARAS DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)**
- **ALARMAS CONTRA ROBO**
- **MEDIDAS CONSTRUCTIVAS EN PAREDES Y VENTANAS**

# 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

## CONTROLES DE ACCESO FÍSICO

### ÁREA DE RECEPCIÓN DE PERSONAS

**CONVIENE ADECUAR UNA ZONA PARA IDENTIFICAR Y ADMITIR O NO A LAS PERSONAS QUE ATRAVIESEN EL PERÍMETRO DE SEGURIDAD**. SE DEBE PERMITIR EL ACCESO A LAS PERSONAS DE UNA EN UNA, TANTO SI SON EMPLEADOS COMO VISITANTES.

LAS ÁREAS DE RECEPCIÓN **DEBERÍAN INCORPORAR BARRERAS FÍSICAS**, COMO PUERTAS, TORNOS, U OTROS. ADEMÁS, SE PRODUCE EL REGISTRO DEL INTENTO DE ACCESO, PARA EL POSTERIOR SERVICIO DE INTELIGENCIA.

SUELEN SER UBICACIONES **IDÓNEAS PARA LA PRESENCIA DE GUARDIAS**, QUE TAMBIÉN DESEMPEÑAN UNA FUNCIÓN INTRÍNSECA DE VIGILANCIA DEL RECINTO.

# 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

## CONTROLES DE ACCESO FÍSICO

### REGISTRO DE ENTRADAS Y SALIDAS

**DEBERÍAN EXISTIR PROCEDIMIENTOS**, DONDE SE **REGISTRE LA FECHA Y HORA DE CADA MOVIMIENTO** A TRAVÉS DEL PERÍMETRO DE SEGURIDAD, INGRESANDO O ABANDONANDO EL RECINTO.

### TRATAMIENTO DE PERSONAL EXTERNO

**EL ACCESO DE PERSONAL SUBCONTRATADO, DE PROVEEDORES O VISITAS**, ES DECIR, DEL PERSONAL AJENO A LA INSTALACIÓN, **REQUIERE UN TRATAMIENTO ESPECIAL**; ASÍ ESTAS TERCERAS PERSONAS **DEBERÍAN SER**:

- IDENTIFICADAS PLENAMENTE.
- CONTROLADAS Y VIGILADAS DURANTE EL ACCESO.

## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

### CONTROLES DE ACCESO FÍSICO

#### GUARDIAS

ESTÁN **UBICADOS EN LUGARES ESTRATÉGICOS DEL PERÍMETRO** MÁS VULNERABLE, COMO SON LAS ENTRADAS Y SALIDAS DEL MISMO. TAMBIÉN DEBE EXISTIR **PERSONAL DE GUARDIA DE LIBRE MOVIMIENTO**, POR EJEMPLO, PARA EL DESEMPEÑO DE LAS FUNCIONES DE ACOMPAÑAMIENTO O ESCOLTA.

#### PUERTAS DE CONTROL ELECTRÓNICO

**EN LA RECEPCIÓN U OTRAS ZONAS A PROTEGER**, SE DEBERÍA INCLUIR UNA PUERTA VALIDABLE POR LA PROPIA PERSONA, **MEDIANTE ALGÚN PROCESO DE AUTENTICACIÓN** O POR OTRA PERSONA, QUE INTERVENGA EN LA AUTENTICACIÓN.

# 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

## CONTROLES DE ACCESO FÍSICO

### ENTRADAS DE DOBLE PUERTA

POR CADA PUERTA SOLO PUEDE PASAR UNA PERSONA. TRAS ACCEDER POR LA PRIMERA PUERTA, ESTA SE CIERRA, QUEDANDO LA PERSONA ATRAPADA Y EXPUESTA, POR EJEMPLO, A UNA CÁMARA DE CIRCUITO CERRADO DE TELEVISIÓN, QUE REGISTRE EL INTENTO DE ACCESO.

A CONTINUACIÓN, SI SE AUTORIZA EL ACCESO, LA SEGUNDA PUERTA DEBE SER ABIERTA, PARA QUE LA PERSONA INGRESE A LAS INSTALACIONES.

# 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

## CONTROLES DE ACCESO FÍSICO

### CÁMARAS DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

EL EMPLEO DE CÁMARAS **PERMITE MONITORIZAR ESPACIOS GRANDES**, Y **CONCENTRAR LA ATENCIÓN EN LOS PUNTOS DE ENTRADA Y SALIDA MÁS VULNERABLES**.

ADEMÁS, DE MANERA INTRÍNSECA, DESEMPEÑAN UNA FUNCIÓN DE REGISTRO DE LOS ACCESOS. DEBERÍAN INSTALARSE DE MANERA DISIMULADA, PARA NO LLAMAR LA ATENCIÓN SOBRE EL VALOR QUE PROTEGEN.

POR EL CONTRARIO, Y, DEBIDO A SU FUNCIÓN DE REGISTRO DE LA IMAGEN, DEBERÍAN INSTALARSE DE MANERA VISIBLE, COMO MEDIDA DISUASORIA DE VANDALISMO U OTROS.

## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

### CONTROLES DE ACCESO FÍSICO

#### ALARMAS CONTRA ROBO

SISTEMAS ELÉCTRICOS Y ELECTRÓNICOS QUE PERMITEN ENVIAR UNA SEÑAL DE **ALARMA CUANDO SE DETECTA UN MOVIMIENTO**, CUANDO SE **ABRE UNA PUERTA O VENTANA**, O CUANDO **SE PRODUCE UNA VIBRACIÓN**.

#### MEDIDAS CONSTRUCTIVAS EN PAREDES Y VENTANAS

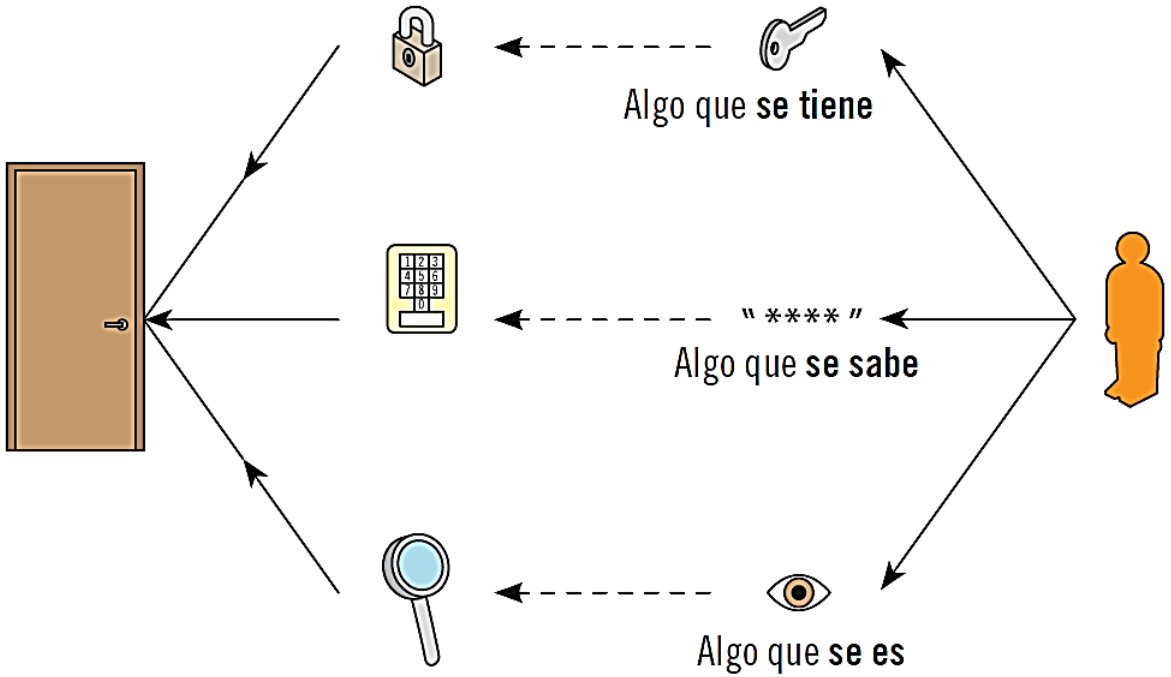
DEBE PRESTARSE ESPECIAL ATENCIÓN A QUE DISPONGAN DE **UNA SÓLIDA CONSTRUCCIÓN**, EVITÁNDOSE PAREDES FALSAS O DÉBILES. EN EL CPD, LAS **PUERTAS Y VENTANAS DEBEN REDUCIRSE** A LAS ESTRICTAMENTE NECESARIAS.

# 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

## MÉTODOS DE IDENTIFICACIÓN DE LAS PERSONAS

**PARA QUE UNA PERSONA SEA IDENTIFICADA, DEBE ENTREGAR ALGO**, Y LOS PARÁMETROS GENERALMENTE EMPLEADOS SON:

- **ALGO QUE SE TIENE**
- **ALGO QUE SE SABE**
- **ALGO QUE SE ES**



## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

### MÉTODOS DE IDENTIFICACIÓN DE LAS PERSONAS

#### ALGO QUE SE TIENE

POR EJEMPLO, UNA LLAVE, UN DOCUMENTO OFICIAL, UNA TARJETA IDENTIFICATIVA MAGNÉTICA, ETC. EL **INCONVENIENTE** DE ESTE MECANISMO ES QUE, CON MAYOR O MENOR ESFUERZO, EL OBJETO **PODRÍA SER COPIADO**.

#### ALGO QUE SE SABE

LO QUE CONLLEVA ALGUNA INFORMACIÓN QUE SOLO CONOCE Y RECUERDA LA PERSONA, COMO UNA CONTRASEÑA, UN CÓDIGO DE ACCESO, O LA RESPUESTA A UNA PREGUNTA PREVIAMENTE CONOCIDA. EL **INCONVENIENTE** DE ESTE MECANISMO ES QUE **LA PERSONA PUEDE REVELAR LA INFORMACIÓN, U OLVIDARLA**.

## 3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS

### MÉTODOS DE IDENTIFICACIÓN DE LAS PERSONAS

#### ALGO QUE SE ES

CONLLEVA **MEDIR ALGUNAS CARACTERÍSTICAS FÍSICAS DE LA PERSONA**, LO QUE SE CONOCE COMO **TÉCNICAS BIOMÉTRICAS**, O MEDIR SUS APTITUDES.

LA IDENTIFICACIÓN CONSISTE EN **TOMAR UNA MEDIDA CON EL LECTOR BIOMÉTRICO, Y COMPARARLA CON EL PATRÓN** (CONOCIDO Y ALMACENADO PREVIA MENTE) DEL INDIVIDUO QUE DICE SER, PARA VERIFICAR O NO LA CONCORDANCIA.

SE EMPLEAN COMO INDICADORES: *LA HUELLA DACTILAR*, *LA GEOMETRÍA DE LA MANO, EL RECONOCIMIENTO DE LA VOZ* REPITIENDO UNA O MÁS FRASES, Y *PATRONES OCULARES DEL IRIS O DE LA RETINA*.

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. **CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS**
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

**LOS CRITERIOS DE SEGURIDAD DEL EMPLAZAMIENTO** CORRESPONDEN EN PRIMER LUGAR A **SU UBICACIÓN**, SI BIEN ES PROBABLE QUE NO SE PUEDAN MODIFICAR, O QUE NO HAYA ALTERNATIVAS, PORQUE LA EMPRESA YA ESTÉ ESTABLECIDA.

PARA REDUCIR LOS RIESGOS DEL EMPLAZAMIENTO, SE PUEDEN DISPONER UN CONJUNTO DE MEDIDAS AMBIENTALES, QUE INTENTEN COMPENSAR LA SEGURIDAD FÍSICA DEL **CPD**.

## 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

### CONSIDERACIONES EN LA LOCALIZACIÓN DEL CPD

**UNA CORRECTA ELECCIÓN EN LA LOCALIZACIÓN DEL CPD**, ES UNA GRAN **SALVAGUARDA PREVENTIVA** PARA MUCHAS AMENAZAS DE ORIGEN NATURAL, DIFÍCILES O COSTOSAS DE COMPENSAR A POSTERIORI.

A CONTINUACIÓN, SE PRESENTAN ALGUNAS **RECOMENDACIONES SOBRE LA LOCALIZACIÓN**, DERIVADAS DE REVISAR LAS AMENAZAS NATURALES, Y ANALIZAR QUÉ CONSIDERACIONES PREVENTIVAS SE PUEDEN ADOPTAR:

- **FRENTE A DESASTRES NATURALES**
- **FRENTE A DESASTRES INDUSTRIALES**
- **FRENTE A LA AMENAZA DE INCENDIO**
- **FRENTE A LA AMENAZA DE INUNDACIÓN**
- **FRENTE A LA AMENAZA DE FALTA DE SUMINISTRO ELÉCTRICO**

# 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

## CONSIDERACIONES EN LA LOCALIZACIÓN DEL CPD

### FRENTE A DESASTRES NATURALES

EL CPD DEBE UBICARSE **LEJOS DE ÁREAS CON FENÓMENOS NATURALES PROBABLES**, COMO: TERREMOTOS, MAREMOTOS, ERUPCIONES VOLCÁNICAS, HURACANES, TORNADOS, TORMENTAS ELÉCTRICAS, INCENDIOS, E INUNDACIONES NATURALES.

### FRENTE A DESASTRES INDUSTRIALES

EL CPD DEBE ESTAR **ALEJADO DE EMPRESAS CON ACTIVIDADES POTENCIALMENTE PELIGROSAS**, COMO INDUSTRIAS QUÍMICAS, AEROPUERTOS, O SUS INMEDIACIONES.

# 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

## CONSIDERACIONES EN LA LOCALIZACIÓN DEL CPD

### FRENTE A LA AMENAZA DE INCENDIO

EL CPD DEBE ESTAR **ALEJADO DE ALMACENES DE PRODUCTOS INFLAMABLES O CON ELEVADO RIESGO DE INCENDIO**, GASOLINERAS, REFINERÍAS, INDUSTRIAS QUÍMICAS, ALMACENES DE PAPEL, TALLERES, HORNOS, ETC. DEBE ESTAR ALEJADO DE LAS CONDUCCIONES DE GAS Y COMBUSTIBLES.

### FRENTE A LA AMENAZA DE INUNDACIÓN

EL CPD DEBE ALEJARSE:

- DEL **CAUCE NATURAL DE RÍOS** CON CAUDAL ACTUAL, O QUE LO TUVIERAN EN EL PASADO.
- DE **RUTAS DE EVACUACIÓN DE PRESAS Y PANTANOS**.
- DE **ZONAS COSTERAS INUNDABLES** O DE POCA ALTITUD.
- DE **TUBERÍAS DE AGUA O DEPÓSITOS DE AGUA**.
- EL CPD **NO DEBERÍA SITUARSE EN SÓTANOS NI EN ÁTICOS**, SINO PREFERIBLEMENTE EN LAS PLANTAS INTERMEDIAS DEL EDIFICIO.

## 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

### CONSIDERACIONES EN LA LOCALIZACIÓN DEL CPD

#### FRENTE A LA AMENAZA DE FALTA DE SUMINISTRO ELÉCTRICO

DEBERÍA UBICARSE EN **EMPLAZAMIENTOS DONDE HAYA SUMINISTRO DE ENERGÍA POR EMPRESAS Y REDES DIFERENTES**; Y A SER POSIBLE, POR RUTAS DE DISTRIBUCIÓN PROCEDENTES DE DOS SUBESTACIONES DIFERENTES.

## 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

### CONTROLES AMBIENTALES DEL CPD

SE DEBERÍAN DISPONER LAS SIGUIENTES **MEDIDAS DE PROTECCIÓN**:

- **EQUIPOS DE CONTROL DE TEMPERATURA Y HUMEDAD**
- **LOS DETECTORES DE AGUA DEBEN UBICARSE EN EL SUELO TÉCNICO**
- **LOS PANELES DE CONTROL DE ALARMAS DEBEN ESTAR SEPARADOS DE LOS SISTEMAS ANTIRROBO O DE SEGURIDAD**
- **DEBEN PROHIBIRSE ACTIVIDADES DENTRO DEL CPD**
- **PLANES DOCUMENTADOS Y PROBADOS DE EVACUACIÓN DURANTE EMERGENCIAS**
- **CONTROLES AMBIENTALES FRENTE A FALLOS**
- **CONTROLES AMBIENTALES PARA INCENDIOS**

## 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

### CONTROLES AMBIENTALES DEL CPD

- **EQUIPOS DE CONTROL DE TEMPERATURA Y HUMEDAD**, Y REVISIONES PERIÓDICAS DEL CPD PARA VERIFICARLO.
- **LOS DETECTORES DE AGUA** DEBEN UBICARSE EN EL SUELO TÉCNICO, Y CERCA DE LOS DESAGÜES, INCLUSO AUNQUE EL CPD SE UBIQUE EN PLANTAS ALTAS, PORQUE EL RIESGO PROCEDE DE CUALQUIER ESCAPE DE AGUA.

## 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

### CONTROLES AMBIENTALES DEL CPD

- **LOS PANELES DE CONTROL DE ALARMAS** DEBEN ESTAR SEPARADOS DE LOS SISTEMAS ANTIRROBO O DE SEGURIDAD. DEBERÍAN ESTAR UBICADOS EN CAJAS HERMÉTICAS, Y EN CONFORMIDAD CON LOS REQUISITOS DE TEMPERATURA DEL FABRICANTE. DEBEN ESTAR ACCESIBLES AL CUERPO DE BOMBEROS, Y EN UNA HABITACIÓN CONTROLADA, QUE IMPIDA EL ACCESO DE TODO EL MUNDO. DEBERÍAN PERMITIR ACTIVAR O DESACTIVAR ZONAS SEPARADAS DENTRO DE LAS INSTALACIONES.
- **DEBEN PROHIBIRSE ACTIVIDADES DENTRO DEL CPD**, COMO EL CONSUMO DE COMIDAS, BEBIDA, Y POR SUPUESTO FUMAR.

## 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

### CONTROLES AMBIENTALES DEL CPD

- **PLANES DOCUMENTADOS Y PROBADOS DE EVACUACIÓN** DURANTE EMERGENCIAS. LOS PLANES DE EVACUACIÓN DEBEN HACER ÉNFASIS EN LA SEGURIDAD HUMANA, PERO NO DEJAR EL CPD FÍSICAMENTE INSEGURO.
- **CONTROLES AMBIENTALES FRENTE A FALLOS ELÉCTRICOS DE CAUSA NATURAL O NO**: PROTECTORES DE VOLTAJE, SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA, GENERADORES, CONMUTADORES DE EMERGENCIA DE ENERGÍA, Y SUMINISTRO ENERGÉTICO REDUNDANTE DESDE DOS SUBESTACIONES.

## 4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS

### CONTROLES AMBIENTALES DEL CPD

- **CONTROLES AMBIENTALES PARA INCENDIOS**: EMPLEO DE DETECTORES DE HUMO, ALARMAS MANUALES, EXTINTORES DE INCENDIOS, SISTEMAS DE SUPRESIÓN, REVISIONES DE ESTOS ELEMENTOS POR INSTALADORES HOMOLOGADOS, O POR EL CUERPO DE BOMBEROS. ADEMÁS, LAS PAREDES, PISO, Y TECHO DEL CPD, DEBEN SER A PRUEBA DE INCENDIOS, EVITANDO SU ENTRADA O SU PROPAGACIÓN, SI EL ORIGEN DEL INCENDIO ES EL PROPIO CPD. LOS MATERIALES DE OFICINA DEBEN SER RESISTENTES AL FUEGO, Y LOS MATERIALES DE LIMPIEZA, NO INFLAMABLES. LOS CABLES DEBEN ESTAR COLOCADOS EN BANDEJAS, PANELES Y CONDUCTOS, TAMBIÉN RESISTENTES AL FUEGO.

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. **EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS**
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

**LA ELECTRICIDAD ES**, DE ENTRE TODOS, **EL COMPONENTE VITAL DE UN CENTRO DE DATOS**.

UNA ANOMALÍA EN EL SUMINISTRO DE ENERGÍA, DE SOLO UNA FRACCIÓN DE SEGUNDO, PUEDE OCASIONAR UN FALLO EN UN SERVIDOR.

SIN SUMINISTRO ELÉCTRICO, LA DISPONIBILIDAD DE LOS SISTEMAS ES NULA, Y SI EL TRÁNSITO **SUMINISTRO-AUSENCIA-SUMINISTRO** NO ESTÁ CONTROLADO, PUEDE VERSE AFECTADA LA INTEGRIDAD DE LA INFORMACIÓN.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## ANOMALÍAS EN EL SUMINISTRO ELÉCTRICO

LAS **TORMENTAS ELÉCTRICAS** Y LAS **TORMENTAS SOLARES** SON FENÓMENOS NATURALES CONOCIDOS, CON **IMPACTO DIRECTO** EN EL SUMINISTRO ELÉCTRICO DE LOS SISTEMAS INFORMÁTICOS.

OTRAS CIRCUNSTANCIAS, COMO **HURACANES, INCENDIOS, ACCIDENTES INDUSTRIALES, O FUERTES VARIACIONES EN LA DEMANDA** DE LOS CONSUMIDORES, TAMBIÉN PUEDEN AFECTAR AL SUMINISTRO.

EN LA PRÁCTICA, SERÁN MÁS FRECUENTES LOS INCIDENTES POR ALGUNA **DEFICIENCIA EN LA INSTALACIÓN ELÉCTRICA**.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## ANOMALÍAS EN EL SUMINISTRO ELÉCTRICO

TODAS ESTAS AMENAZAS SE TRADUCEN EN LAS SIGUIENTES ANOMALÍAS DEL SUMINISTRO ELÉCTRICO:

- **INTERRUPCIONES DEL SUMINISTRO**
- **CAÍDAS DE TENSIÓN**
- **PICOS Y VALLES DE TENSIÓN**
- **INTERFERENCIAS ELECTROMAGNÉTICAS O RUIDO ELÉCTRICO**
- **CORRIENTE ESTÁTICA**

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## ANOMALÍAS EN EL SUMINISTRO ELÉCTRICO

### INTERRUPCIONES DEL SUMINISTRO

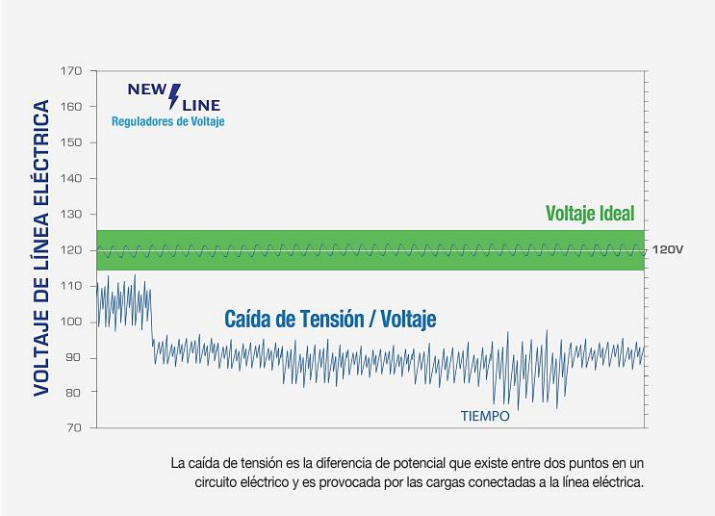
CONLLEVAN LA PÉRDIDA COMPLETA DEL SUMINISTRO, Y SUELEN AFECTAR A ÁREAS MEDIANAS (EDIFICIO), O GRANDES (UNA CIUDAD COMPLETA). ENTRE LAS CAUSAS MÁS FRECUENTES ESTÁN LAS TORMENTAS ELÉCTRICAS, Y LA PROPIA INCAPACIDAD DE SUMINISTRO DEL PROVEEDOR.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## ANOMALÍAS EN EL SUMINISTRO ELÉCTRICO

### CAÍDAS DE TENSIÓN

EL SUMINISTRO ELÉCTRICO ES MUY INFERIOR AL ESPERADO, GENERALMENTE POR PROBLEMAS DE CAPACIDAD DEL PROVEEDOR, O POR DEFECTOS EN LA INSTALACIÓN PROPIA. GENERAN UN DAÑO IRREVERSIBLE A LOS EQUIPOS, QUE SE VEN FORZADOS A TRABAJAR POR DEBAJO DE SUS LÍMITES PREVISTOS, LO QUE SE PUEDE CUANTIFICAR EN UNA REDUCCIÓN DE SU VIDA ÚTIL.



La caída de tensión es la diferencia de potencial que existe entre dos puntos en un circuito eléctrico y es provocada por las cargas conectadas a la línea eléctrica.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## ANOMALÍAS EN EL SUMINISTRO ELÉCTRICO

### PICOS Y VALLES DE TENSIÓN

EL SUMINISTRO DE ENERGÍA ALTERNA SUPERA AMPLIAMENTE SUS MÁXIMOS Y SUS MÍNIMOS. GENERA UN DAÑO IRREVERSIBLE, ACORTANDO LA VIDA ÚTIL Y, EN CASOS EXTREMOS, PRODUCIRÁ SU DESTRUCCIÓN INMEDIATA, E INCLUSO SU INCENDIO. SON PROPENSOS A SUFRIR ESTAS SOBRE- TENSIONES LAS LÍNEAS DE MUCHO RECORRIDO, TANTO DE SUMINISTRO ELÉCTRICO, COMO DE TELEFONÍA, QUE CON GRANDES LONGITUDES FORMAN UNA EXTENSA MALLA DE INTERCONEXIÓN ENTRE DIFERENTES EDIFICIOS.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## ANOMALÍAS EN EL SUMINISTRO ELÉCTRICO

### INTERFERENCIAS ELECTROMAGNÉTICAS O RUIDO ELÉCTRICO

GENERADAS POR TORMENTAS GEOMAGNÉTICAS (SOLARES), ASÍ COMO APARATOS ELÉCTRICOS O ELECTRÓNICOS; ESPECIALMENTE AQUELLOS CON GRANDES CONSUMOS Y QUE INCORPORAN BOBINAS, TRANSFORMADORES Y REACTANCIAS, COMO MOTORES, TUBOS FLUORESCENTES, MÁQUINAS DE AIRE ACONDICIONADO, O SISTEMAS CON RELÉS, QUE CONLLEVEN BRUSCAS VARIACIONES DE LA CORRIENTE CONSUMIDA.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## ANOMALÍAS EN EL SUMINISTRO ELÉCTRICO

### CORRIENTE ESTÁTICA

SE TRATA DE CORRIENTE DE MUY POCA INTENSIDAD, PERO ALTÍSIMO VOLTAJE, INDUCIDO O CONDUCIDO POR LA PERSONA, DE MANERA QUE, AUNQUE ESTA NO SUFRA NINGÚN DAÑO, EL ORDENADOR SUFRE UNA DESCARGA DE MILES DE VOLTIOS, SUFICIENTE PARA DESTROZAR SUS COMPONENTES (MEMORIA, DISCO DURO, PROCESADOR, ETC.). FRECUENTEMENTE OLVIDADA, PUEDE INDUCIRSE SIMPLEMENTE TOCANDO CON LA MANO LA PARTE METÁLICA DEL EQUIPO, ACARREANDO SU DESTRUCCIÓN COMPLETA.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## MEDIDAS PARA GARANTIZAR EL SUMINISTRO ELÉCTRICO

LA INSTALACIÓN ELÉCTRICA DE UN CPD ES UNA LABOR COMPLEJA, Y QUE PRECISA DE PERSONAL EXPERTO EN INSTALACIONES ELÉCTRICAS. LAS **MEDIDAS MÁS HABITUALES** PARA LAS AMENAZAS VISTAS:

- **INTERRUPCIONES DEL SUMINISTRO**
- **CAÍDAS DE TENSIÓN**
- **SOBRETENSIONES (PICOS Y VALLES)**
- **INTERFERENCIAS Y RUIDO**
- **CUADRO ELÉCTRICO DE PROTECCIÓN**

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## MEDIDAS PARA GARANTIZAR EL SUMINISTRO ELÉCTRICO

### INTERRUPCIONES DEL SUMINISTRO

PARA PODER SUPERAR INTERRUPCIONES BREVES, DE SEGUNDOS O INCLUSO DE ALGÚN MINUTO, SE DEBEN DISPONER **SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (O SAI),** CAPACES DE MANTENER EL SUMINISTRO ELÉCTRICO DURANTE UN TIEMPO CORTO. LOS SAI TIENEN **COMO PARÁMETROS FUNDAMENTALES**):

- SU **CAPACIDAD** EN "KILOVOLTIOS X AMPERIO" O "KVA" PERMITE CALCULAR LA POTENCIA Y CORRIENTE MÁXIMA QUE PUEDE ENTREGAR.
- SU **AUTONOMÍA**, MINUTOS U HORAS, PARA UN SUMINISTRO CONTINUO A SU CAPACIDAD MÁXIMA.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## MEDIDAS PARA GARANTIZAR EL SUMINISTRO ELÉCTRICO

### CAÍDAS DE TENSIÓN

SE EMPLEARÁN **PROTECTORES DE VOLTAJE** EN LOS CUADROS DE PROTECCIÓN ELÉCTRICA.

### SOBRETENSIONES (PICOS Y VALLES)

NUEVAMENTE, SE INTEGRARÁN **PROTECTORES DE VOLTAJE**, INTEGRADOS EN **LOS CUADROS DE PROTECCIÓN ELÉC**TRICA DEL RECINTO, Y TAMBIÉN **LOS SAI** CORREGIRÁN EL SUMINISTRO ELÉCTRICO, Y PROTEGERÁN A LOS EQUIPOS.

# 5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS

## MEDIDAS PARA GARANTIZAR EL SUMINISTRO ELÉCTRICO

### INTERFERENCIAS Y RUIDO

DISPONER DE UNA BUENA CONEXIÓN DE **TOMA DE TIERRA**. TAMBIÉN SE EMPLEAN **FILTROS ESPECÍFICOS PARA INTERFERENCIAS**. UNA MEDIDA CONSTRUCTIVA PARA EL CPD, SUELE SER COLOCAR EN LA CONSTRUCCIÓN DE SUS PAREDES, SUELO Y TECHO, UNA MALLA METÁLICA CONECTADA A TIERRA QUE HAGA LAS VECES DE **JAULA DE FARADAY**.

### CUADRO ELÉCTRICO DE PROTECCIÓN

UN **CUADRO ELÉCTRICO BIEN DIMENSIONADO, IDENTIFICADO, Y CONSTRUIDO**, ES LA PRIMERA CONTRAMEDIDA FRENTE A LOS PROBLEMAS DE SUMINISTRO, APARTE DE LA NECESARIA PROTECCIÓN QUE DEBE APORTAR A LAS PERSONAS FRENTE A DESCARGAS

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. **REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS**
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

EL **SEGUNDO FACTOR VITAL EN UN CPD**, DESPUÉS DEL SUMINISTRO ELÉCTRICO, ES SU CLIMA, EN TÉRMINOS DE **TEMPERATURA Y HUMEDAD**.

**LOS EQUIPOS DEBEN OPERAR SIEMPRE EN LAS CONDICIONES MARCADAS POR EL FABRICANTE**, Y EXCEDERLAS CONLLEVARÁ LA REDUCCIÓN ACELERADA DE LA VIDA ÚTIL, EL MALFUNCIONAMIENTO, Y LA DESTRUCCIÓN DEL EQUIPO.

POR ÚLTIMO, POR SU ALTO RIESGO, DEBIDO A LA ELEVADA DENSIDAD DE EQUIPOS ELECTRÓNICOS Y FUERTE CONSUMO ELÉCTRICO, **RESULTA ESPECIALMENTE IMPORTANTE LA PREVENCIÓN DE INCENDIOS**.

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## CLIMATIZACIÓN

LOS EQUIPOS QUE SE ACUMULAN EN UN CPD TIENEN UN ELEVADO CONSUMO ELÉCTRICO, QUE CONLLEVA UNA ELEVADA DISIPACIÓN DE CALOR.

ADEMÁS, LA DENSIDAD DE EQUIPOS QUE PUEDEN ALOJARSE EN UN CPD ES CADA VEZ MAYOR, DADA LA CRECIENTE TENDENCIA A REDUCIR EL TAMAÑO DE LOS EQUIPOS.

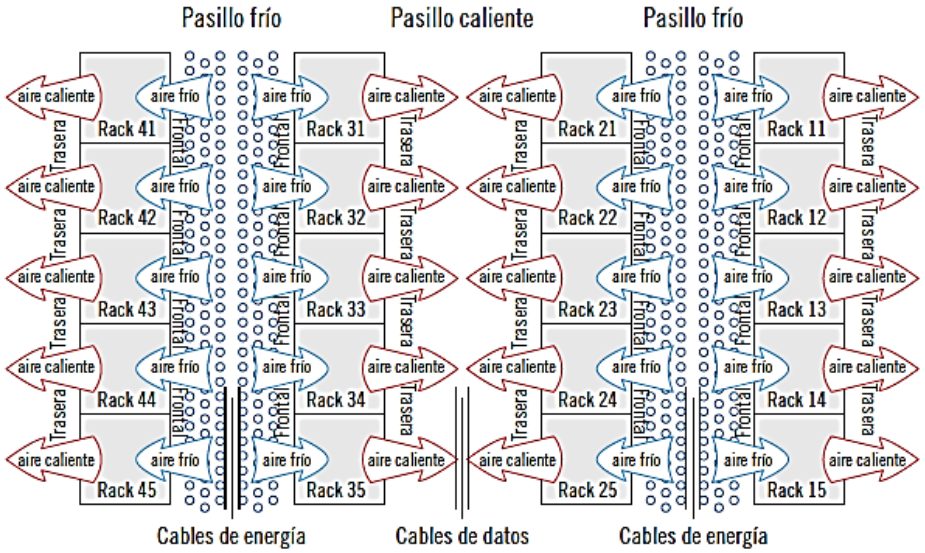
EL RESULTADO ES QUE EN **EL CPD SE ACUMULARÁ UNA ELEVADA CANTIDAD DE CALOR, QUE SE DEBE GESTIONAR**.

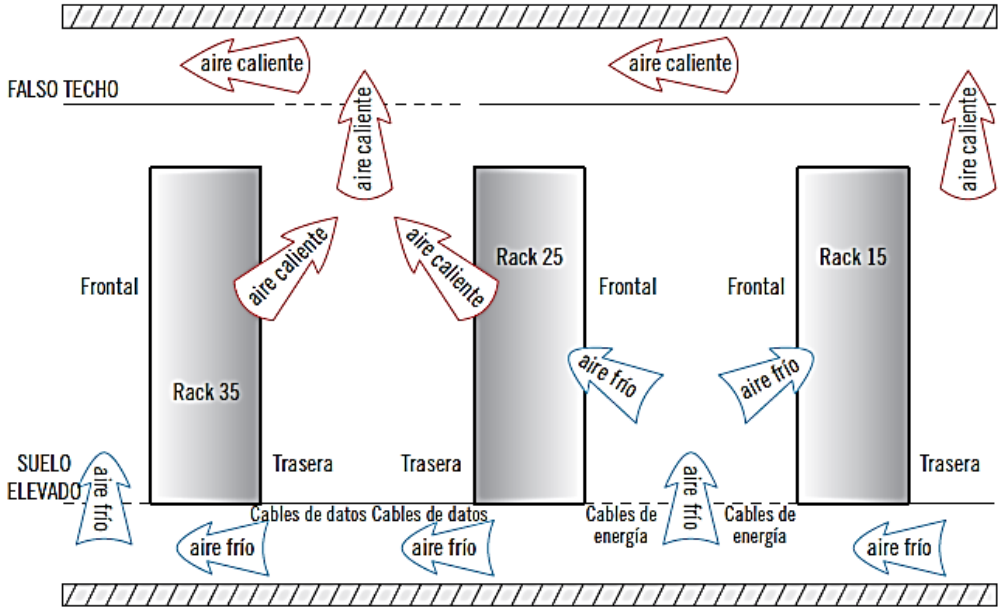
# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## CLIMATIZACIÓN

PARA CONTROLAR LA TEMPERATURA EXISTEN DOS CONSIDERACIONES:

- **ELEMENTOS DE REFRIGERACIÓN**
- **UNA ADECUADA CIRCULACIÓN DEL AIRE**



# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## CLIMATIZACIÓN

### ELEMENTOS DE REFRIGERACIÓN

SIN LOS CUALES NO SE PUEDE MANTENER BAJO CONTROL Y DE MANERA ESTABLE LA TEMPERATURA.

LA TEMPERATURA CENTRAL ES IMPORTANTE, PERO MANTENERLA ESTABLE DE MANERA QUE HAYA PEQUEÑAS VARIACIONES TAMBIÉN ES MUY IMPORTANTE, **PORQUE LOS COMPONENTES ELECTRÓNICOS SON MUY SENSIBLES A LOS CAMBIOS DE TEMPERATURA**, TANTO MÁS CUANTO MÁS BRUSCOS SEAN.

COMO NORMA GENERAL, **SUELEN EMPLEARSE MÁRGENES DE OPERACIÓN, DE 18º– 24º C.**

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## CLIMATIZACIÓN

### ADECUADA CIRCULACIÓN DEL AIRE

QUE REDUNDARÁ EN LA EFICIENCIA DEL EQUIPO DE REFRIGERACIÓN, TANTO MÁS CUANTO MAYOR SEA EL CPD.

**PARA SEPARAR EL AIRE CALIENTE DEL AIRE FRÍO, Y FACILITAR LA CIRCULACIÓN**, SE EMPLEA EL CONCEPTO DE **PASILLOS CALIENTES Y PASILLOS FRÍOS.**

NO MENOS IMPORTANTE ES CONTROLAR LA HUMEDAD RELATIVA, VINCULADA AL CALOR EMITIDO POR LOS EQUIPOS Y A SU REFRIGERACIÓN, COMO SE EXPLICA A CONTINUACIÓN. **SUELEN SER RANGOS NORMALES ENTRE EL 30 % Y EL 55 % DE HUMEDAD RELATIVA**.

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## PROTECCIÓN CONTRA INCENDIOS

LA PROTECCIÓN FRENTE A INCENDIOS EN UN CPD PRESENTA DOS PECULIARIDADES FRENTE A OTROS RECINTOS:

- **UN CPD ESTÁ OCUPADO MAYORITARIAMENTE POR MATERIAL ELECTRÓNICO DELICADO**
- **LOS EQUIPOS DEL CPD ESTÁN ALIMENTADOS ELÉCTRICAMENTE**

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## PROTECCIÓN CONTRA INCENDIOS

### UN CPD ESTÁ OCUPADO MAYORITARIAMENTE POR MATERIAL ELECTRÓNICO DELICADO

QUE DEBERÍA EVITAR SOMETERSE A MECANISMOS DE EXTINCIÓN QUE LO DAÑARAN (COMO EL POLVO O ALGUNOS AGENTES QUÍMICOS), ASÍ COMO AGENTES DE EXTINCIÓN QUE REDUJERAN MUY BRUSCAMENTE SU TEMPERATURA (COMO LA EXTINCIÓN POR CO O NIEVE CARBÓNICA), YA QUE EL MATERIAL ELECTRÓNICO PUEDE QUEDAR DESTRUIDO POR BRUSCOS CAMBIOS DE TEMPERATURA.

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## PROTECCIÓN CONTRA INCENDIOS

### LOS EQUIPOS DEL CPD ESTÁN ALIMENTADOS ELÉCTRICAMENTE

ES POSIBLE ENCONTRAR FUEGO DE ORIGEN ELÉCTRICO, LO QUE IMPIDE EMPLEAR AGUA, U OTROS AGENTES EXTINTORES CONDUCTORES DE LA ELECTRICIDAD, COMO ALGUNAS ESPUMAS.

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## PROTECCIÓN CONTRA INCENDIOS

LAS MEDIDAS DE PROTECCIÓN QUE EXISTEN SON:

- **PAREDES, TECHOS, Y SUELOS A PRUEBA DE INCENDIOS**
- **PUERTA CON SUFICIENTE GRADO DE PROTECCIÓN FRENTE AL FUEGO**
- **DETECTORES DE HUMO**
- **ALARMAS DE INCENDIO MANUALES**
- **EXTINTORES DE INCENDIO MANUALES**
- **SISTEMAS DE EXTINCIÓN DE INCENDIO AUTOMÁTICO**

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## PROTECCIÓN CONTRA INCENDIOS

### PAREDES, TECHOS, Y SUELOS A PRUEBA DE INCENDIOS

QUE CIERREN EL RECINTO. NO DEBE EXISTIR COMUNICACIÓN POR SUELOS NI TECHOS CON LOS RECINTOS CERCANOS. NO DEBEN PERMITIR LA ENTRADA DE FUEGO, NI PROPAGARLO SI SE ORIGINARA DENTRO.

### PUERTA CON SUFICIENTE GRADO DE PROTECCIÓN FRENTE AL FUEGO

NO DEBE PERMITIR LA ENTRADA DE FUEGO, NI PROPAGARLO SI SE ORIGINARA DENTRO.

### DETECTORES DE HUMO

QUE SE DEBEN SITUAR EN EL FALSO TECHO, QUE ES DONDE PRIMERO SE ACUMULARÁ EL HUMO. DEBERÍAN ESTAR CONECTADAS A UNA ALARMA AUDIBLE, Y SER PRACTICABLES PARA SU MANTENIMIENTO.

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## PROTECCIÓN CONTRA INCENDIOS

### ALARMAS DE INCENDIO MANUALES

LOCALIZADAS EN SITIOS ESTRATÉGICOS, GENERALMENTE CERCA DE PUERTAS Y SALIDAS DE EMERGENCIA. DEBERÍAN ESTAR CONECTADAS A UNA ALARMA AUDIBLE.

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## PROTECCIÓN CONTRA INCENDIOS

### EXTINTORES DE INCENDIO MANUALES.

NOTA: **EL FUEGO DE UN INCENDIO** SE CLASIFICA EN **CUATRO TIPOS**, EN FUNCIÓN DEL COMBUSTIBLE:

- **FUEGO TIPO A**, QUE ES EL QUE SE PRODUCE EN COMBUSTIBLES SÓLIDOS COMUNES, COMO MADERA, PAPELES, CARTONES, TEXTILES, PLÁSTICOS, ETC. DEJAN RESIDUOS EN FORMA DE BRASAS O CENIZAS.
- **FUEGO TIPO B**: ES EL QUE SE PRODUCE EN COMBUSTIBLES LÍQUIDOS INFLAMABLES, COMO GASOLINA, PINTURAS, GAS LICUADO DE PETRÓLEO, O ALGUNAS GRASAS LUBRICANTES. NO DEJAN RESIDUOS AL QUEMARSE.
- **FUEGO TIPO C**, COMÚNMENTE DENOMINADOS “FUEGO ELÉCTRICO”, ES EL QUE SE PRODUCE EN EQUIPOS O INSTALACIONES CON CARGA ELÉCTRICA. ESTE ES EL CASO DE UN FUEGO QUE SE DESARROLLA EN UN CPD.
- **FUEGO TIPO D**, QUE SE PRODUCE EN METALES, COMO VIRUTAS DE ALEACIONES DE ALUMINIO, MAGNESIO, U OTROS.

# 6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS

## PROTECCIÓN CONTRA INCENDIOS

### SISTEMAS DE EXTINCIÓN DE INCENDIO AUTOMÁTICO

ESTOS SISTEMAS SE ACTIVAN DE MANERA AUTOMÁTICA, CUANDO DETECTAN UNA ALTA TEMPERATURA. LOS SISTEMAS AUTOMÁTICOS BASADOS EN AGUA (POR EJEMPLO, EMPLEANDO ROCIADORES), NO SON ADECUADOS, POR LA INCOMPATIBILIDAD ELÉCTRICA. LOS ADECUADOS PARA INSTALACIONES DE CPD SON BASADOS EN GASES PRESURIZADOS QUE, UNA VEZ LIBERADOS, DESPLAZAN EL OXÍGENO DEL AIRE, EXTINGUIENDO EL FUEGO.

ESTOS SISTEMAS DEBEN SER DESCARGADOS MANUALMENTE, INTRODUCIENDO POR TANTO UNA DEMORA EN LA EXTINCIÓN, Y PUEDEN ACARREAR OTRAS ACCIONES, COMO EL CIERRE DE PUERTAS, O EL CORTE DEL SUMINISTRO ELÉCTRICO. DEBEN CONECTARSE A UNA ALARMA AUDIBLE, CON ANTELACIÓN A LA LIBERACIÓN DEL AGENTE EXTINTOR, PARA QUE EL PERSONAL PUEDA ABANDONAR EL RECINTO.

SE DEBEN CHEQUEAR AL MENOS ANUALMENTE, Y REALIZAR PRUEBAS, AUNQUE SEAN PARCIALES. EN NINGÚN CASO DEBE EMPLEARSE CO, YA QUE ESTE GAS NO SOSTIENE LA VIDA HUMANA, POR ESO LAS INSTALACIONES QUE PUEDAN LIBERAR CO CON PRESENCIA HUMANA SON ILEGALES.

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. **ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN**
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN

LAS MEDIDAS PARA DOTAR UN **CPD** DE SF PUEDEN SER COSTOSAS EN TÉRMINOS ECONÓMICOS. CONVIENE RECORDAR QUE LA IMPLANTACIÓN DE SALVAGUARDAS DEBE SER PROPORCIONAL A LOS RIESGOS EXISTENTES, E IR PRECEDIDA DE UN ANÁLISIS DE RIESGOS.

LA **NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL DE LA EMPRESA** DEBERÍA **RECOGER AL MENOS LA LEGISLACIÓN APLICABLE, LAS NORMAS DE REFERENCIA EMPLEADAS, Y LAS MEDIDAS APLICADAS**.

A CONTINUACIÓN, SE PROPONE UN ÍNDICE DE LOS CONTENIDOS QUE DEBERÍAN DESARROLLARSE EN UNA NORMATIVA APOYADA EN LA NORMA **ISO 27002.**

## 7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN

### NORMATIVA DE SEGURIDAD FÍSICA

#### A. LEGISLACIÓN APLICABLE

- REGLAMENTO DE DESARROLLO DE LA LOPD (ART.99, CONTROL DE ACCESO FÍSICO).
- ESQUEMA NACIONAL DE SEGURIDAD (ART. 17, MEDIDAS DE PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS).
- NORMA BÁSICA DE EDIFICACIÓN SOBRE PROTECCIÓN DE INCENDIOS (NCB-CPI96).
- REGLAMENTO DE INFRAESTRUCTURAS COMUNES DE TELECOMUNICACIONES (ICT).
- REGLAMENTO ELECTROTÉCNICO DE BAJA TENSIÓN (RBT).

## 7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN

### NORMATIVA DE SEGURIDAD FÍSICA

#### B. NORMAS DE REFERENCIA

- INTERFERENCIA ELECTROMAGNÉTICA (EMI) Y COMPATIBILIDAD ELECTROMAGNÉTICA (EMC).
- UNE EN 50174, DE INSTALACIÓN DEL CABLEADO.
- TIA568B, DE ESTÁNDAR DE CABLEADO.
- TIA942, DE DISEÑO DE DATACENTER.
- ISO17779, PARA LA PRÁCTICA DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

# 7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN

## NORMATIVA DE SEGURIDAD FÍSICA

### C. MEDIDAS APLICADAS EN LA EMPRESA, ACORDES CON LA NORMA ISO 27002

- C1 PERÍMETRO DE SEGURIDAD FÍSICA
- C2 CONTROLES FÍSICOS DE ENTRADA
- C3 SEGURIDAD DE LAS OFICINAS, DESPACHOS E INSTALACIONES
- C4 PROTECCIÓN PARA AMENAZAS EXTERNAS Y DE ORIGEN AMBIENTAL
- C5 TRABAJO EN ÁREAS SEGURAS
- C6 ÁREAS DE ACCESO PÚBLICO Y DE CARGA Y DESCARGA
- C7 EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS
- C8 INSTALACIONES DE SUMINISTRO
- C9 SEGURIDAD EN EL CABLEADO
- C10 MANTENIMIENTO DE EQUIPOS
- C11 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES
- C12 REUTILIZACIÓN O RETIRADA SEGURA
- C13 SALIDA DE MATERIALES

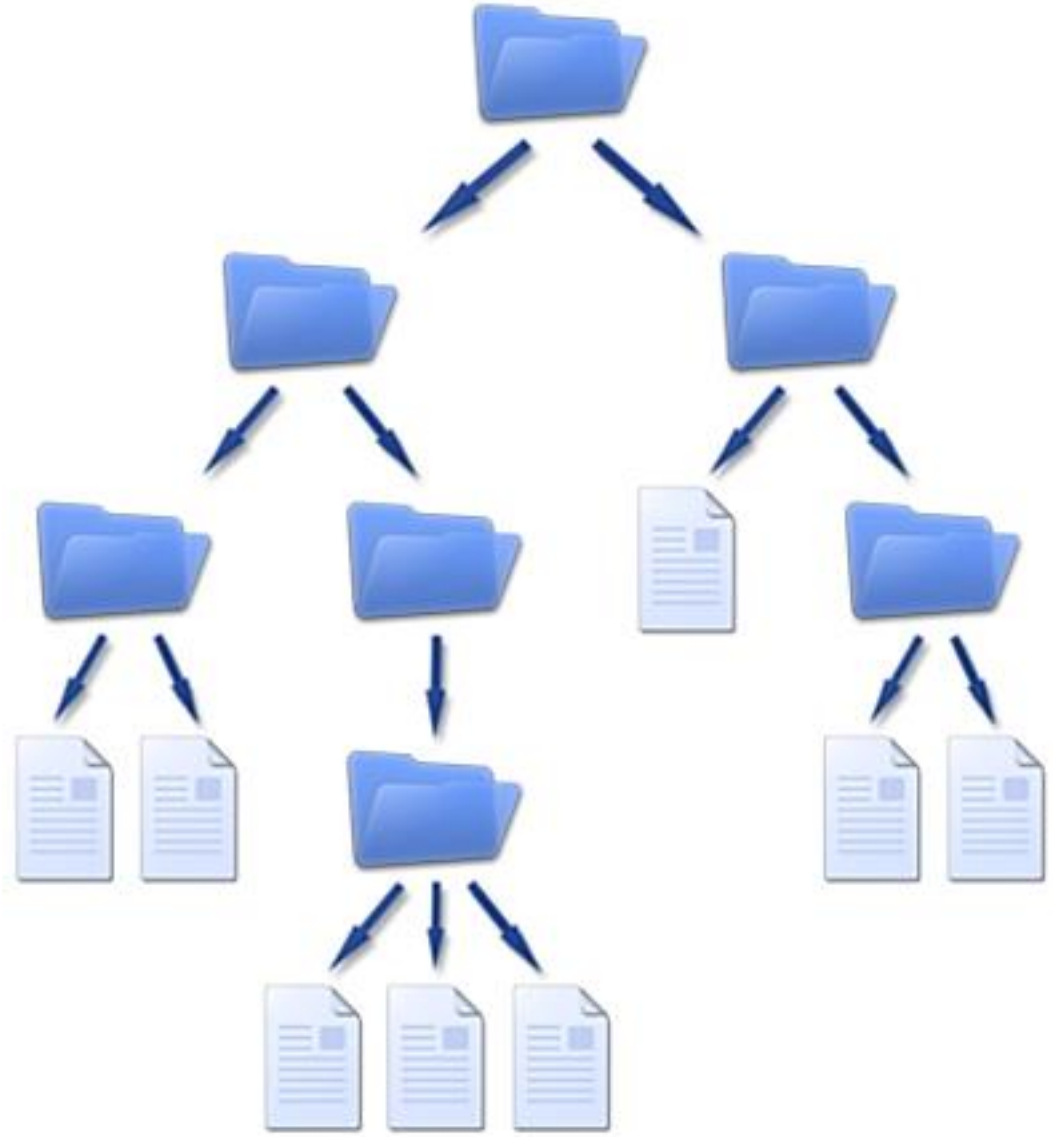
# CONTENIDOS

**Comienza con este epígrafe el estudio de la Seguridad Lógica**

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. **SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS**
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS

EL **SISTEMA DE ARCHIVOS** ES UN ELEMENTO VITAL PARA EL SISTEMA DE INFORMACIÓN Y SU SEGURIDAD, PORQUE LIMITA CÓMO SE DIVIDIRÁ EN FICHEROS EL ACTIVO DE INFORMACIÓN, Y CÓMO SE GESTIONARÁN ESTAS UNIDADES ELEMENTALES DE VALOR.



## 8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS

### FICHEROS

**INFORMACIÓN** ES LA COMUNICACIÓN O ADQUISICIÓN DE CONOCIMIENTOS QUE PERMITEN AMPLIAR O PRECISAR LOS QUE SE POSEEN SOBRE UNA MATERIA DETERMINADA.

PARA PODER ALMACENARLA Y TRANSMITIRLA, LA INFORMACIÓN SE DEBE TRADUCIR A NÚMEROS, MEDIANTE UN PROCESO DE **CODIFICACIÓN**.

LA CODIFICACIÓN DEBE SER REVERSIBLE, MEDIANTE EL PROCESO DE **DECODIFICACIÓN**.

# 8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS

## FICHEROS

TANTO LA CODIFICACIÓN COMO LA DECODIFICACIÓN DEBEN SEGUIR MECANISMOS O CONVENCIONES CONOCIDAS POR QUIENES SE QUIERAN INTERCAMBIAR INFORMACIÓN.

LOS NÚMEROS QUE REPRESENTAN LA INFORMACIÓN SE LLAMARÁN **DATOS**.

UNA VEZ QUE SE TIENE LA INFORMACIÓN TRADUCIDA A DATOS, SE PUEDE AUTOMATIZAR SU PROCESAMIENTO, ALMACENARLA, TRANSMITIRLA, ENCRIPTARLA, SACAR UNA COPIA, ETC.

UN **FICHERO** ES UN CONJUNTO DE DATOS, CON AL MENOS UN NOMBRE ASOCIADO. EL NOMBRE SE NECESITA PARA PODER DISTINGUIR UN FICHERO DE OTRO.

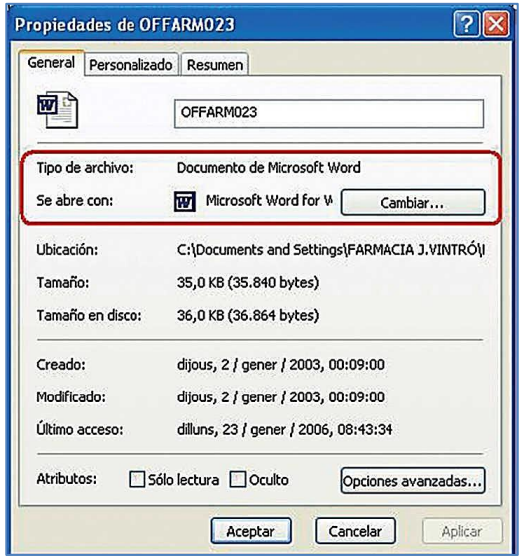
# 8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS

## FICHEROS

ESTE CONJUNTO DE DATOS, ADEMÁS DEL NOMBRE, NECESITARÁ TENER OTRAS MUCHAS **PROPIEDADES**, ENTRE OTRAS:

- *LA FECHA DE CREACIÓN*
- *EL PROPIETARIO DEL FICHERO*
- *INFORMACIÓN SOBRE QUIÉN PUEDE LEERLO, MODIFICARLO, O ELIMINARLO*
- *LA FECHA DE LA ÚLTIMA ESCRITURA, ETC.*

TODAS ESTAS PROPIEDADES SON NECESARIAS PARA PODER ORGANIZAR DE MANERA EFICAZ UN CONJUNTO ELEVADO, Y GENERALMENTE CRECIENTE, DE FICHEROS.



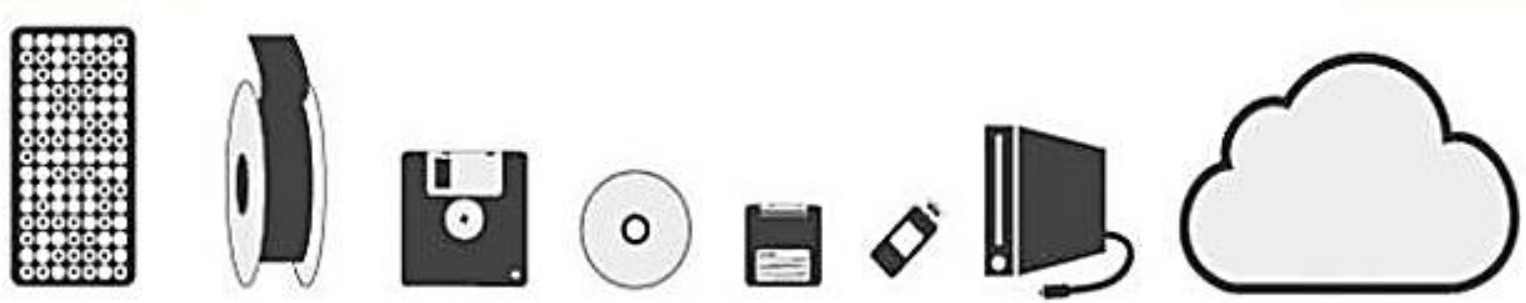
# 8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS

## FICHEROS

LOS FICHEROS SE ALMACENAN EN **MEDIOS DE ALMACENAMIENTO**, EXISTIENDO UNA AMPLIA VARIEDAD DE TECNOLOGÍAS, ALGUNAS DE LOS CUALES SON:

- MEDIOS MAGNÉTICOS.
- MEDIOS ÓPTICOS.
- MEDIOS DE ESTADO SÓLIDO, O SEMICONDUCTORES.

LOS FICHEROS PUEDEN TENER DIFERENTES PROPIEDADES, Y SE PUEDEN DISEÑAR DIVERSOS MÉTODOS PARA GESTIONAR LAS PROPIEDADES Y LOS PROPIOS FICHEROS.



# 8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS

## FICHEROS

UN **SISTEMA DE FICHEROS** ES LA ESPECIFICACIÓN DE TODOS LOS ASPECTOS QUE RESULTEN NECESARIOS PARA ADMINISTRAR LOS FICHEROS EN UN MEDIO DE ALMACENAMIENTO

AL FICHERO TAMBIÉN SE LE DENOMINA **ARCHIVO**, PUDIÉNDOSE EMPLEAR AMBOS TÉRMINOS DE MANERA INTERCAMBIABLE CASI SIEMPRE.

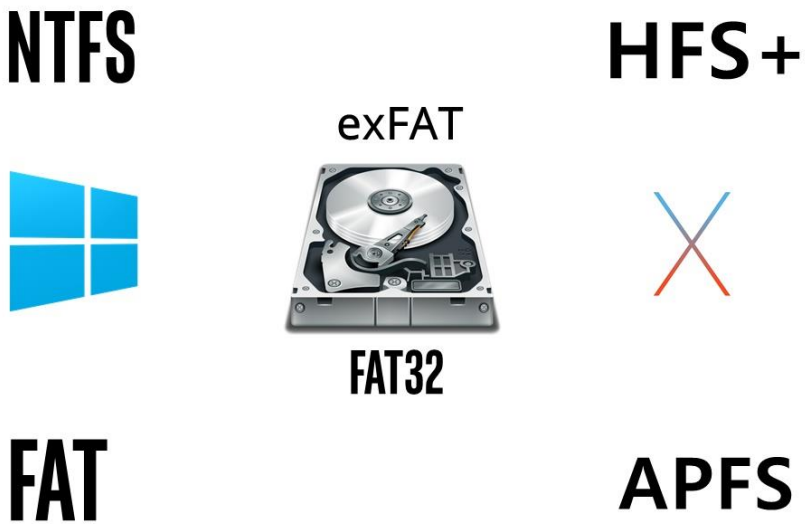
DE LA MISMA MANERA, AL SISTEMA DE FICHEROS SE LE DENOMINA COMÚNMENTE **SISTEMA DE ARCHIVOS**.

# 8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS

## FICHEROS

LOS PRINCIPALES TIPOS SISTEMAS DE ARCHIVOS QUE ENCONTRAMOS SON LOS SIGUIENTES:

- **NTFS** (NEW TECHNOLOGY FILE SYSTEM).
- **HPFS** (HIGH PERFORMANCE FILE SYSTEM).
- **EXT** (EXTENDED FILE SYSTEM).
- **HFS+** (HIERARCHICAL FILE SYSTEM).
- **APFS** (APPLE FILE SYSTEM).
- **FAT** (FILE ALLOCATION TABLE).
- **EXFAT** (EXTENDED FILE ALLOCATION)
- **FAT32**



# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. **ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN**
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

LA **SL** SE OCUPA DE LAS BARRERAS, PROCEDIMIENTOS, Y MECANISMOS PARA MANTENER EL **RESGUARDO E INTEGRIDAD DE LOS ACTIVOS FÍSICOS O LÓGICOS** DE LA EMPRESA, DE FORMA QUE **SOLO SE PERMITA ACCEDER LÓGICAMENTE A ELLOS** A LAS PERSONAS AUTORIZADAS PARA HACERLO.

LA NORMA **ISO 27002** DEDICA SU **CAPÍTULO 9** POR COMPLETO **AL CONTROL DE ACCESO** LÓGICO CON LOS SIGUIENTES OBJETIVOS:

- **LIMITAR EL ACCESO** A LOS RECURSOS DE TRATAMIENTO DE INFORMACIÓN Y A LA INFORMACIÓN.
- **GARANTIZAR EL ACCESO DE USUARIOS AUTORIZADOS** Y EVITAR EL ACCESO NO AUTORIZADO A LOS SISTEMAS Y SERVICIOS.
- PARA **QUE LOS USUARIOS SE HAGAN RESPONSABLES** DE SALVAGUARDAR SU INFORMACIÓN DE AUTENTICACIÓN.
- **PREVENIR EL ACCESO NO AUTORIZADO** A LOS SISTEMAS Y APLICACIONES.

## 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

SE TRATA DE PROTEGER FRENTE A ACCESOS NO AUTORIZADOS Y ATAQUES LÓGICOS, Y PARA ELLO, EL PRINCIPAL ELEMENTO ES EL **CONTROL DE ACCESO LÓGICO** (**CAL**).

LOS **CAL** ESTÁN MÁS RELACIONADOS CON LOS MECANISMOS DE SEGURIDAD IMPLEMENTADOS EN EL PROPIO SISTEMA DE INFORMACIÓN, QUE CON LA DISTRIBUCIÓN DE LA INFORMACIÓN A TRAVÉS DE REDES.

EL **CAL** SE OCUPA DE LOS PROCESOS DE **IDENTIFICACIÓN, AUTENTICACIÓN, Y AUTORIZACIÓN. DEL CORRECTO ESTABLECIMIENTO DE ESTOS TRES PROCESOS SE OBTENDRÁ UNA SEGURIDAD LÓGICA ADECUADA**, QUE ASEGURE QUE SOLO LOS USUARIOS IDENTIFICADOS Y AUTENTICADOS ACCEDEN A LOS RECURSOS AUTORIZADOS.

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## IDENTIFICACIÓN Y AUTENTICACIÓN

LA **IDENTIFICACIÓN** ES EL PROCESO POR EL QUE UNA PERSONA DICE **QUIÉN ES**.

LA **AUTENTICACIÓN** ES EL PROCESO POR EL QUE SE COMPRUEBA QUE UNA PERSONA **ES QUIEN DICE SER**.

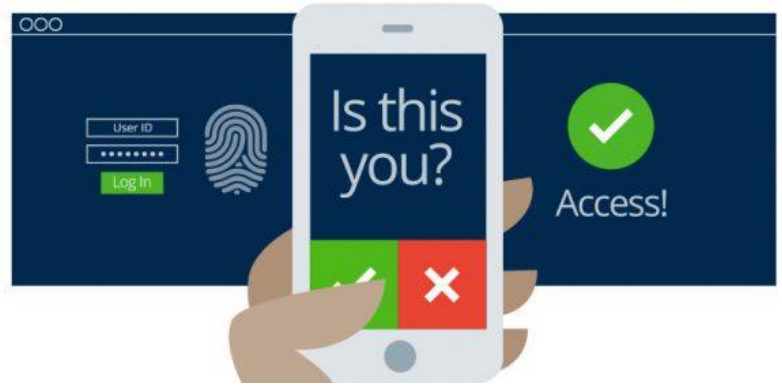
**LA IDENTIFICACIÓN Y LA AUTENTICACIÓN PROTEGEN EL ACCESO AL SISTEMA.**

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## IDENTIFICACIÓN Y AUTENTICACIÓN

EN LA **IDENTIFICACIÓN**, *EL USUARIO PRESENTA AL SISTEMA SU IDENTIDAD*, NORMALMENTE EN LA FASE DE INICIO DE SESIÓN.

EN LA FASE DE **AUTENTICACIÓN**, *SE DEBE VERIFICAR QUE EL USUARIO IDENTIFICADO ESTÁ CONSIDERADO COMO VÁLIDO POR EL SISTEMA,* PARA LO QUE DEBE DEMOSTRAR QUE ESTÁ EN POSESIÓN DE CREDENCIALES QUE PERMITAN COMPROBAR SU AUTENTICIDAD.



# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## IDENTIFICACIÓN Y AUTENTICACIÓN

NORMALMENTE, SE EMPLEAN SISTEMAS BASADOS EN:

- **ALGO QUE SOLAMENTE EL USUARIO CONOCE** (UNA CONTRASEÑA)
- **ALGO QUE EL USUARIO POSEE** (UNA TARJETA INTELIGENTE O SMARTCARD)
- **ALGO QUE EL USUARIO ES** (COMO LOS SISTEMAS BIOMÉTRICOS, UNA FIRMA MANUSCRITA O UNA PRUEBA DE VOZ).

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## IDENTIFICACIÓN Y AUTENTICACIÓN

ESTOS DOS PROCESOS PERMITIRÍAN DISCRIMINAR EXCLUSIVAMENTE QUIÉN PUEDE ACCEDER AL SISTEMA, PERO NO PROTEGER SUS ELEMENTOS INDIVIDUALES.

PARA ESTO SE PRECISA LA **AUTORIZACIÓN**, QUE DIFERENCIA LOS RECURSOS INDIVIDUALMENTE, Y QUIÉN ESTÁ AUTORIZADO A REALIZAR QUÉ COSA SOBRE ELLOS

**LA AUTORIZACIÓN PROTEGE EL USO DE LOS RECURSOS DEL SISTEMA.**

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## AUTORIZACIÓN

LA **AUTORIZACIÓN** ES EL **PROCESO POR EL QUE SE COMPRUEBA SI SE PUEDE LLEVAR A CABO UNA ACCIÓN SOBRE UN RECURSO**.

SE TRATA DE EVALUAR LA CONCESIÓN DE PRIVILEGIOS A UN USUARIO QUE TIENE GARANTÍA DE SER AUTÉNTICO, SEGÚN EL ESTADO ACTUAL DEL SISTEMA.

LA AUTORIZACIÓN, ADEMÁS DEL RECURSO, PUEDE INCLUIR RESTRICCIONES DE TIEMPO, O DE LA ACCIÓN CONCRETA SOBRE EL RECURSO.

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## AUTORIZACIÓN

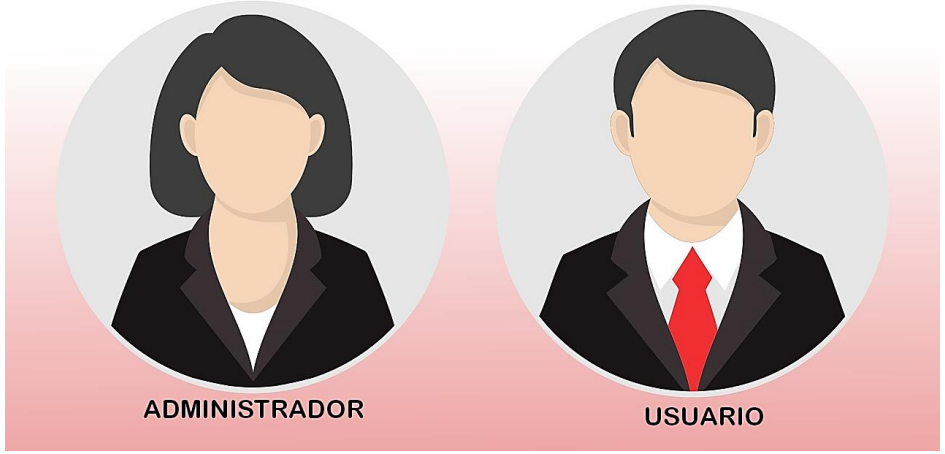
EXISTEN VARIOS MODOS DE AUTORIZACIÓN:

- **CONTROL DE ACCESO DISCRECIONAL (DACL),** EN EL QUE ES EL PROPIETARIO DEL RECURSO EL QUE DETERMINA QUIÉN PUEDE ACCEDER AL MISMO Y QUÉ ACCIONES PUEDE REALIZAR.
- **CONTROL DE ACCESO MANDATORIO (MAC),** DONDE ES EL PROPIO SISTEMA QUIEN PROTEGE LOS RECURSOS.
- **CONTROL DE ACCESO BASADO EN ROLES (RBAC),** QUE INTENTA AUNAR LOS MÉTODOS ANTERIORES: EL SISTEMA ES QUIEN TIENE LA AUTORIDAD PARA DECIDIR EL CONTROL DE ACCESOS, PERO NO EMPLEA ETIQUETAS, SINO ROLES BASADOS EN LOS REQUISITOS FUNCIONALES DE LA ACTIVIDAD QUE REALIZA LA PERSONA.

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## ESTABLECIMIENTO DEL CONTROL DE ACCESOS

PARA ESTABLECER UN CAL, SE PRECISAN VARIOS ELEMENTOS, Y LO PRIMERO ES DEFINIR UNOS **USUARIOS** *QUE PUEDAN ACREDITAR SU IDENTIDAD, MEDIANTE UN SECRETO COMPARTIDO SOLO CON EL SISTEMA*, DE MANERA QUE EL SISTEMA PUEDA COMPROBAR SI TIENEN AUTORIZADO EL ACCESO AL RECURSO QUE SOLICITAN.

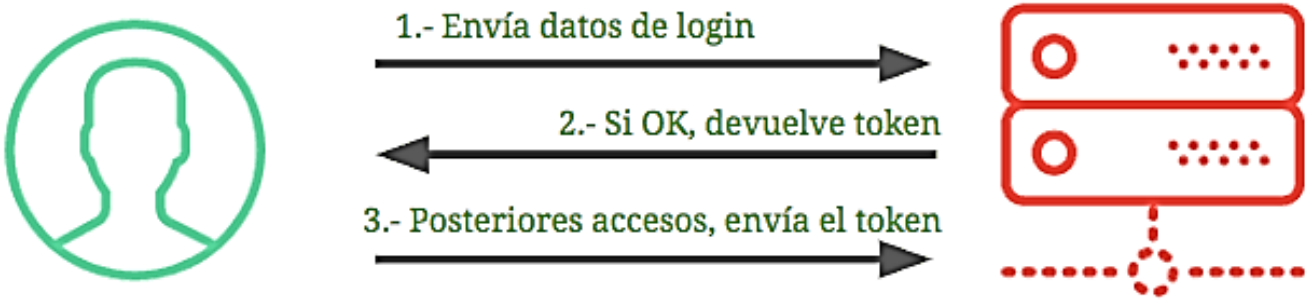


# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## ESTABLECIMIENTO DEL CONTROL DE ACCESOS

### USUARIOS

UN **USUARIO ES TODA PERSONA QUE PUEDE HACER USO DE CUALQUIER RECURSO DEL SISTEMA**. LA REPRESENTACIÓN LÓGICA DEL USUARIO EN EL SISTEMA DE INFORMACIÓN SERÁ UN CONJUNTO DE INFORMACIÓN, QUE AL MENOS CONSISTIRÁ EN UN **NOMBRE** (LOGIN) Y **UNA INFORMACIÓN**, QUE SOLO DEBE SER COMPARTIDA POR LA PERSONA Y POR EL SISTEMA, EN BASE A LA QUE PODER REALIZAR LA AUTENTICACIÓN.



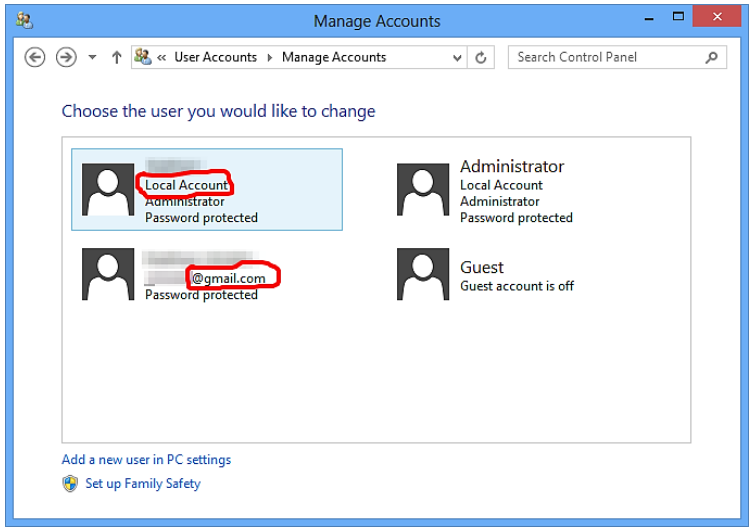
# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## ESTABLECIMIENTO DEL CONTROL DE ACCESOS

### USUARIOS

LA ENTIDAD USUARIO TENDRÁ OTRA INFORMACIÓN. TODA ESTA INFORMACIÓN SOBRE EL USUARIO, SU FICHA, SE AGRUPA EN LO QUE SE DENOMINA **CUENTA DE USUARIO**.

LOS USUARIOS SE GESTIONAN MEDIANTE CUENTAS DE USUARIO, QUE DEBEN SER ACCESIBLES DESDE CUALQUIER ORDENADOR DE LA RED.



# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## ESTABLECIMIENTO DEL CONTROL DE ACCESOS

### USUARIOS

LA GESTIÓN DE LAS CUENTAS DE USUARIO DEBE REALIZARSE DE MANERA CENTRALIZADA. SE LLEVA A CABO EN UN SERVIDOR DE CUENTAS DE USUARIO O SERVIDOR DE DIRECTORIO (AL CONJUNTO DE CUENTAS SE LE DENOMINA **DIRECTORIO DE USUARIOS O DIRECTORIO**).

EXISTEN DIVERSAS SOLUCIONES TECNOLÓGICAS QUE ENTREGAN ESTE SERVICIO DE DIRECTORIO, Y EXISTEN NORMAS INTERNACIONALES QUE DEFINEN ESTE SERVICIO, SIENDO ALTAMENTE RECOMENDABLE QUE EL SERVICIO DE DIRECTORIO ELEGIDO SEA COMPATIBLE CON EL **PROTOCOLO LDAP**.

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## ESTABLECIMIENTO DEL CONTROL DE ACCESOS

### SERVICIO DE DIRECTORIO

LOS SERVICIOS DE DIRECTORIO **SE EXTIENDEN PARA CONTENER NO SOLO LA INFORMACIÓN DE LAS CUENTAS DE USUARIO, SINO LA DE OTROS ELEMENTOS** QUE LAS APLICACIONES PUEDAN NECESITAR CONOCER DESDE CUALQUIER UBICACIÓN DE LA RED.

**SE ALMACENAN LOS NOMBRES DE LOS ORDENADORES**, **LAS CARPETAS COMPARTIDAS**, DE LOS **SERVIDORES DE IMPRESIÓN**, **DE CORREO ELECTRÓNICO**, Y CUALQUIER OTRA INFORMACIÓN PARA LA GESTIÓN DE LA PROPIA RED, COMO ALGUNAS CONFIGURACIONES DE PERSONALIZACIÓN DE LOS USUARIOS O DE LOS ORDENADORES.

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## ESTABLECIMIENTO DEL CONTROL DE ACCESOS

### SERVICIO DE DIRECTORIO

EN SISTEMAS **MICROSOFT WINDOWS,** LA SOLUCIÓN IMPLEMENTADA SE DENOMINA **DIRECTORIO ACTIVO** (**ACTIVE DIRECTORY**).

CUANDO SE INSTALA EL **SERVICIO DE AD EN UN SERVIDOR**, DICHO SERVIDOR **SE CONVIERTE EN UN CONTROLADOR DE DOMINIO, Y EL RESTO DE LOS ORDENADORES** DE LA RED PUEDEN CONVERTIRSE **EN SUS CLIENTES**, RECIBIENDO TODA LA INFORMACIÓN DEL **AD**.

**EL CONJUNTO DE ORDENADORES** QUE COMPARTEN UN SERVICIO DE DIRECTORIO **SE DENOMINA DOMINIO**.

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## ESTABLECIMIENTO DEL CONTROL DE ACCESOS

### SERVICIO DE AUTENTICACIÓN

EL **SERVIDOR DEL DIRECTORIO** LLEVA A CABO LA AUTENTICACIÓN, YA CONTIENE LA BASE DE DATOS DE USUARIOS Y LA INFORMACIÓN PARA SU AUTENTICACIÓN.

LAS APLICACIONES DEBEN SABER CÓMO INICIAR UNA SOLICITUD DE AUTENTICACIÓN, Y CÓMO INTERPRETAR LA RESPUESTA CUANDO SEA POSITIVA O NEGATIVA, ETC.

PARA ELLO, **SE DEFINEN LOS PROTOCOLOS DE AUTENTICACIÓN**, QUE GOBIERNAN ESTAS COMUNICACIONES.

# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## ESTABLECIMIENTO DEL CONTROL DE ACCESOS

### SERVICIO DE AUTENTICACIÓN

LOS **SISTEMAS MICROSOFT WINDOWS** EMPLEAN EL **PROTOCOLO *KERBEROS***, Y EN **LINUX, *OPENLDAP*** TAMBIÉN LO ADMITE.

**EN CADA INTENTO DE ACCESO** A UN FICHERO, **SE COMPRUEBA SI EL** IDENTIFICADOR DEL **USUARIO** (YA AUTENTICADO) **ESTÁ O NO INCLUIDO EN LA ACL** QUE EL SISTEMA DE FICHEROS TIENE DEFINIDO, Y QUÉ ACCIONES CONCRETAS PUEDE REALIZAR EL USUARIO.

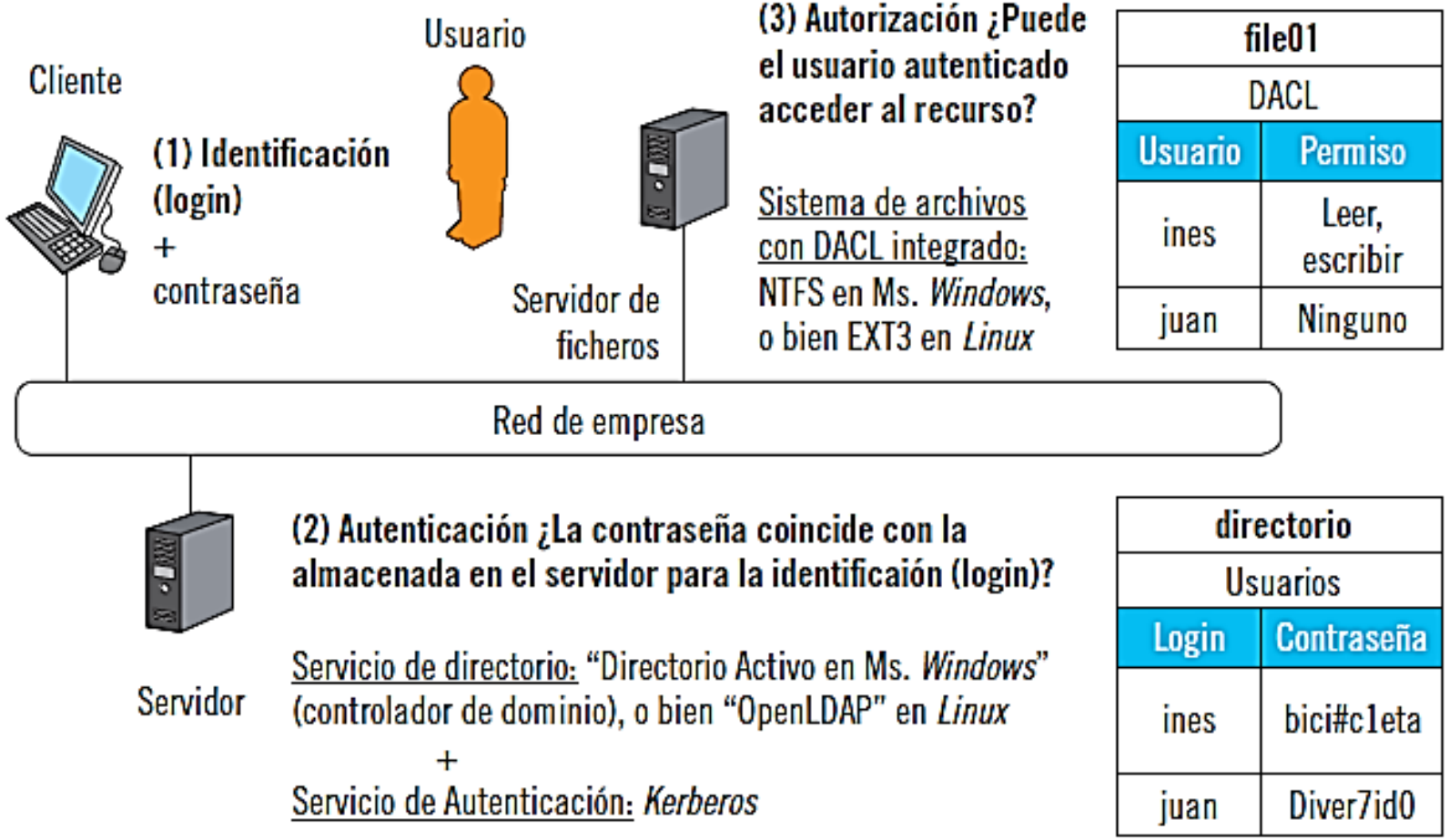
# 9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN

## RESUMEN DE LOS ELEMENTOS QUE INTERVIENEN EN EL CONTROL DE ACCESO LÓGICO

**(1 ) IDENTIFICACIÓN**

**(2) AUTENTICACIÓN**

**(3) AUTORIZACIÓN**




| file01 | |
|---|---|
| DACL | |
| **Usuario** | **Permiso** |
| ines | Leer, escribir |
| juan | Ninguno |

| directorio | |
|---|---|
| Usuarios | |
| **Login** | **Contraseña** |
| ines | bici#c1eta |
| juan | Diver7id0 |

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. **CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS**
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 10.CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS

EL **DIRECTORIO DE USUARIOS** ES EL CONJUNTO DE INFORMACIÓN QUE **PERMITIRÁ GESTIONAR DE MANERA CENTRALIZADA** TODOS LOS ASPECTOS DE LOS **ELEMENTOS LÓGICOS** DE LA RED DE LA EMPRESA, ESPECIALMENTE LAS CUENTAS DE USUARIO.

SERÍA DESEABLE QUE ESTA CONFIGURACIÓN PUDIERA APLICARSE NO INDIVIDUALMENTE A CADA USUARIO, SINO DE MANERA MÁS AMPLIA, A UN CONJUNTO O **GRUPO DE USUARIOS.**

## 10.CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS

SERÍA DESEABLE QUE ESTAS CONFIGURACIONES SE PUDIERAN GESTIONAR DE MANERA INDEPENDIENTE A LOS USUARIOS A LOS QUE SE LES APLICA.

EL **DIRECTORIO ACTIVO (AD)** LO PERMITE, EXTENDIENDO EL SERVICIO DE DIRECTORIO CON EL CONCEPTO DE **POLÍTICAS DE GRUPO (GPO, GROUP POLICY OBJECT).**

LAS **GPO** SON OBJETOS DEL DIRECTORIO ACTIVO QUE TIENE COMO ATRIBUTOS CADA UNA DE LAS POLÍTICAS (**DIRECTIVAS**) QUE PUEDE ESTABLECERSE.

EXISTEN **DOS TIPOS DE DIRECTIVAS**, SEGÚN AFECTEN A LOS USUARIOS, O A LOS EQUIPOS.

## 10.CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS

LAS **GPO** SE CONFIGURAN PARA **APLICARLAS SOBRE TODO EL DOMINIO**, **O SOBRE UN SUBCONJUNTO** DE ESTE (**UNIDAD ORGANIZATIVA OU**).

GENERALMENTE, LAS DIRECTIVAS SE APLICAN A LAS **OU,** QUE PUEDEN CONTENER TANTOS USUARIOS COMO EQUIPOS.

LAS DIRECTIVAS DE USUARIO DE LA **GPO** SE APLICARÁN A LOS USUARIOS CONTENIDOS EN LA **OU** CUANDO ESTOS INICIAN SESIÓN EN CUALQUIER EQUIPO DEL DOMINIO; Y LAS DIRECTIVAS DE EQUIPO SE APLICARÁN A LOS EQUIPOS DE LA OU CADA VEZ QUE ESTOS SE INICIEN.

## 10.CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS

CADA **GPO** CONTIENE UN ÁRBOL DE POLÍTICAS, QUE SE DIVIDE EN DIRECTIVAS DE CONFIGURACIÓN DE EQUIPO Y DIRECTIVAS DE CONFIGURACIÓN DE USUARIO. A SU VEZ, CADA DIRECTIVA SE SUBDIVIDE EN TRES GRUPOS:

- **CONFIGURACIÓN DE SOFTWARE**
- **CONFIGURACIÓN DE WINDOWS**
- **PLANTILLAS ADMINISTRATIVAS**

# 10.CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS

**CONFIGURACIÓN DE SOFTWARE**

PERMITE DEFINIR ASPECTOS RELACIONADOS CON LA INSTALACIÓN AUTOMÁTICA DEL MISMO.

**CONFIGURACIÓN DE WINDOWS**

DEFINE PARÁMETROS DEL SISTEMA OPERATIVO COMO LOS PARÁMETROS DE SEGURIDAD, SECUENCIAS DE COMANDOS A EJECUTAR EN EL INICIO DE SESIÓN, O PARÁMETROS DE SEGURIDAD.

**PLANTILLAS ADMINISTRATIVAS**

SON LAS CONFIGURACIONES QUE SE GUARDAN EN EL REGISTRO DE WINDOWS, RELACIONADAS CON EL FUNCIONAMIENTO Y APARIENCIA DEL ESCRITORIO, Y DE MUCHOS COMPONENTES DEL SISTEMA OPERATIVO LOCAL.

# 10.CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS

## POLÍTICAS DE SEGURIDAD

ENTRE LAS POLÍTICAS DE SEGURIDAD MÁS RELEVANTES, SE ENCUENTRAN SIN DUDA LAS REFERENTES A LAS DIRECTIVAS DE LAS CONTRASEÑAS, LAS OPCIONES DE AUDITORÍA Y LA CONFIGURACIÓN DE LOS REGISTROS QUE DEBEN REALIZARSE:

- **POLÍTICAS DE CUENTAS**
- **POLÍTICAS LOCALES**
- **REGISTRO DE EVENTOS**

# 10.CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS

## POLÍTICAS DE CUENTAS

SE PUEDEN CONFIGURAR LOS PERIODOS DE CADUCIDAD DE LAS CONTRASEÑAS, LAS CONDICIONES DE BLOQUEO DE LAS CUENTAS, LA CONFIGURACIÓN DE KERBEROS, ETC.

## POLÍTICAS LOCALES

SE CONFIGURAN AQUÍ LAS OPCIONES DE AUDITORÍA, Y ASIGNACIÓN DE DERECHOS Y PRIVILEGIOS DE USUARIO.

## REGISTRO DE EVENTOS

SE CONTROLA EL REGISTRO DE EVENTOS DEL SISTEMA, EN LAS CATEGORÍAS DEL VISOR DE SUCESOS PARA EL REGISTRO DE APLICACIÓN, EL REGISTRO DE SEGURIDAD, Y EL REGISTRO DEL SISTEMA.

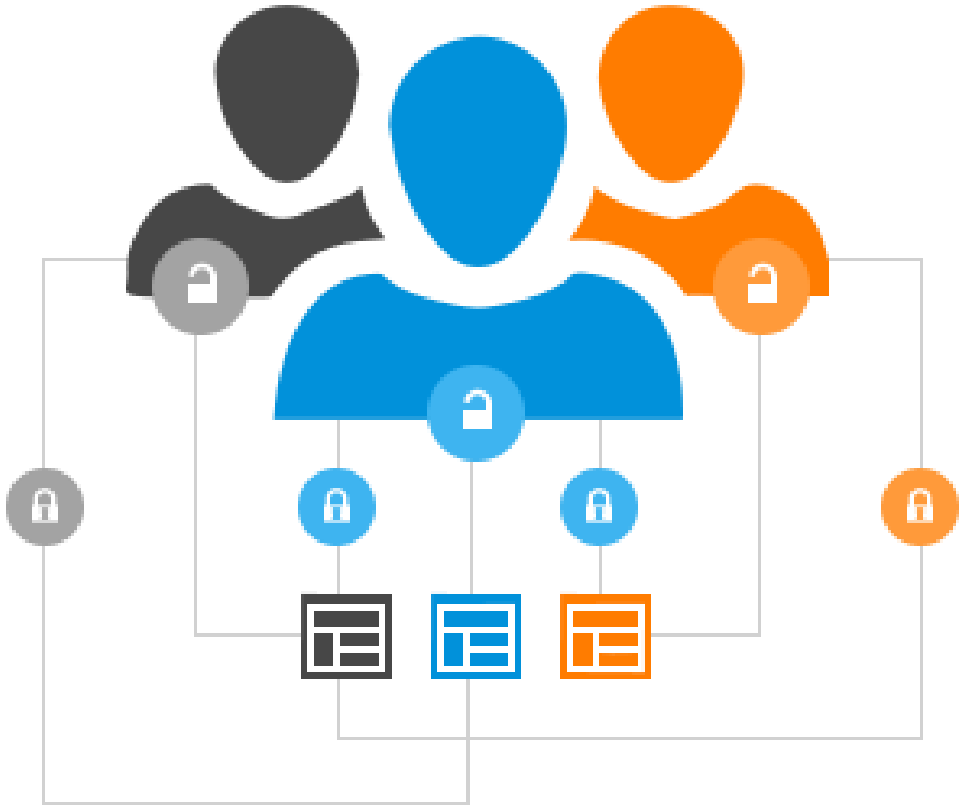
# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. **ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS**
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

# 11.ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS

LAS **LISTAS DE CONTROL DE ACCESO** PARA UN FICHERO O DIRECTORIO **DEFINEN QUÉ USUARIOS AUTENTICADOS PUEDEN ACCEDER AL FICHERO, Y QUÉ TAREAS PUEDEN REALIZAR.**

NORMALMENTE LOS PERMISOS DE ACCESO SE PUEDEN ESTABLECER A NIVEL DE UN USUARIO CONCRETO, O DE UN GRUPO DE USUARIOS, LO QUE FACILITA ENORMEMENTE LA GESTIÓN DE ESTOS PERMISOS.



# 11.ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS

## ACL POR USUARIO O POR GRUPOS DE USUARIOS

CUANDO UN FICHERO TIENE CONFIGURADO PERMISO DE ACCESO DETERMINADO PARA UN GRUPO Y SE QUIERE QUE UN NUEVO USUARIO TAMBIÉN PUEDA ACCEDER AL MISMO, HABRÍA DOS POSIBILIDADES:

- AGREGAR A LA **ACL** DEL FICHERO EL PERMISO PARA EL NUEVO USUARIO
- AGREGAR EL USUARIO AL GRUPO DE USUARIOS.

LA ELECCIÓN DE UNA OPCIÓN U OTRA DEPENDERÁ PRINCIPALMENTE DE LO DIVERSIFICADOS QUE SEAN LOS PERMISOS DE ACCESO.

EN GENERAL, RESULTA MÁS ADECUADO OTORGAR PERMISOS DE MANERA INDIRECTA, MEDIANTE LA INCLUSIÓN O EXCLUSIÓN DE LOS USUARIOS EN LOS GRUPOS.

# 11.ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS

## PROPIETARIO

LOS SISTEMAS DE FICHEROS APLICAN EL CONCEPTO DE PROPIETARIO.

**EL PROPIETARIO DE UN FICHERO** ES SU CREADOR, Y HABITUALMENTE DISPONDRÁ DE PERMISOS FUNCIONALES COMPLETOS. NO OBSTANTE, INCLUSO EL PROPIETARIO DE UN FICHERO PUEDE CARECER DE OTROS PERMISOS ESPECIALES.

ES FRECUENTE QUE ESTOS PERMISOS ESPECIALES, RELACIONADOS CON LA SEGURIDAD DEL SISTEMA (POR EJEMPLO, EL **NO REPUDIO**, DERIVADO DE LA INCAPACIDAD DE NO PODER CAMBIAR UN PROPIETARIO), ESTÉN EXCLUSIVAMENTE LIMITADOS AL ADMINISTRADOR, O A UN GRUPO DE ADMINISTRADORES.

# 11.ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS

## HERENCIA

LOS SISTEMAS DE FICHEROS PUEDEN VISUALIZARSE COMO UNA ESTRUCTURA JERÁRQUICA EN FORMA DE ÁRBOL INVERTIDO. ESTOS SISTEMAS INCORPORAN EL CONCEPTO DE **HERENCIA**, ES DECIR, LOS ACL QUE SE DEFINEN EN LOS NIVELES SUPERIORES, SE AÑADEN AUTOMÁTICAMENTE A LOS ACL DE LOS ELEMENTOS DE NIVELES INFERIORES.

EL MECANISMO DE HERENCIA TAMBIÉN PUEDE INTERRUMPIRSE EN CUALQUIER NIVEL DE LA JERARQUÍA, DE MANERA QUE LOS ACL DEJARÍAN DE AÑADIRSE AUTOMÁTICAMENTE A LOS ELEMENTOS DE NIVELES INFERIORES.

## 11.ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS

AUNANDO EL CONCEPTO DE PROPIETARIO Y EL DE HERENCIA SOBRE UN RECURSO COMPARTIDO POR RED, SE PUEDE CONSTRUIR UNA VERSIÓN MÍNIMA DE UN SISTEMA DE INTERCAMBIO DE ARCHIVOS, QUE ASEGURE LA CONFIDENCIALIDAD Y LA INTEGRIDAD DE LOS DATOS.

SIN EMBARGO, CONVIENE DISPONER DE MEDIDAS DE CONTROL ADICIONALES, COMO LA **ASIGNACIÓN DE CUOTAS** PARA QUE EL EXCESO DE CONSUMO DE UN USUARIO NO PENALICE AL RESTO, NI SUPONGA UNA AMENAZA DE AGOTAMIENTO DE LOS RECURSOS QUE PODRÍA CONLLEVAR A LA DETENCIÓN DEL SISTEMA.

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. **GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS**
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## 12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS

**EL INFRACTOR MÁS HABITUAL ES EL ACCIDENTAL**, QUE GENERA EL INCIDENTE POR ERROR, O SIN SABER LO QUE ESTÁ HACIENDO.

ADEMÁS DE APLICAR MEDIDAS DE CONTROL DE ACCESO A LOS FICHEROS PARA SU PROTECCIÓN, **SE DEBE MANTENER BAJO CONTROL CUÁLES SON LOS USUARIOS DEL SISTEMA.**

LOS SISTEMAS INCORPORAN HERRAMIENTAS PARA LA ADECUADA GESTIÓN TÉCNICA.

## 12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS

EL PROBLEMA MÁS HABITUAL ES QUE **EL CONJUNTO DE USUARIOS DEBE MANTENERSE ACTUALIZADO**, LO QUE PRECISA DE UNA REGULAR SUPERVISIÓN HUMANA ADEMÁS DE UNOS CLAROS Y ESTRICTOS PROCEDIMIENTOS DE ALTAS Y BAJAS DE USUARIOS.

## 12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS

EN UNA **RED WINDOWS**, CON SU INFORMACIÓN ORGANIZADA EN TORNO A UN **DIRECTORIO ACTIVO**, SE EMPLEA EL CONCEPTO DE USUARIO GLOBAL AL DOMINIO, PARA REPRESENTAR LÓGICAMENTE A LAS PERSONAS QUE PODRÍAN ACCEDER A LOS RECURSOS DESDE CUALQUIER PUNTO DE LA RED.

LOS DATOS, ALMACENÁNDOSE EN EL DIRECTORIO ACTIVO, SON CONOCIDOS POR TODOS LOS ORDENADORES DEL DOMINIO.

ESTE CONCEPTO DIFIERE DEL DE USUARIO LOCAL, CUYO ÁMBITO DE ACCIÓN SE LIMITA AL DEL ORDENADOR DONDE SE CREE EL USUARIO.

LA GESTIÓN DE USUARIOS ES MUY SENCILLA, DESDE EL INTERFAZ GRÁFICO DE WINDOWS, EMPLEANDO LA HERRAMIENTA ADMINISTRATIVA USUARIOS Y EQUIPOS DEL DIRECTORIO.

Active Directory

## 12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS

LA CREACIÓN DE USUARIOS EN LINUX ES IGUALMENTE SENCILLA. DEPENDIENDO DE LA IMPLEMENTACIÓN LDAP, SE EMPLEARÁN UNAS HERRAMIENTAS O NO. EL ADMINISTRADOR DEL SISTEMA PUEDE CREAR LOS USUARIOS Y LOS GRUPOS DE USUARIOS.

CADA USUARIO DEBE PERTENECER AL MENOS A UN GRUPO, Y LOS USUARIOS DE UN GRUPO SE CLASIFICAN EN **ADMINISTRADORES DEL GRUPO** (QUE PUEDEN DAR DE ALTA Y BAJA OTROS INTEGRANTES DEL GRUPO,) Y MIEMBROS DEL GRUPO.

EL SISTEMA INCORPORARA LOS COMANDOS ESTÁNDAR: **ADDUSER**, **USERDEL**, **GROUPADD**, Y **CHAGE**.

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. **REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO**
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

# 13.REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO

SE RECOMIENDA AJUSTARSE A LO DISPUESTO POR LA NORMA **ISO 27002**, QUE INCLUYE EL OBJETIVO 9.4. **CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**, PARA EVITAR EL ACCESO NO AUTORIZADO A LOS SISTEMAS Y APLICACIONES, Y FIJA LOS OBJETIVOS:

- SE DEBERÍA RESTRINGIR EL ACCESO A LA INFORMACIÓN Y A LAS FUNCIONES DE LAS APLICACIONES, DE ACUERDO CON LA POLÍTICA DE CONTROL DE ACCESO DEFINIDA.
- CUANDO ASÍ SE REQUIERA EN LA POLÍTICA DE CONTROL DE ACCESO, EL ACCESO A LOS SISTEMAS Y A LAS APLICACIONES SE DEBERÍA CONTROLAR POR MEDIO DE UN PROCEDIMIENTO SEGURO DE INICIO DE SESIÓN.
- LOS SISTEMAS PARA LA GESTIÓN DE CONTRASEÑAS DEBERÍAN SER INTERACTIVOS Y ESTABLECER CONTRASEÑAS SEGURAS Y ROBUSTAS.
- SE DEBERÍA RESTRINGIR Y CONTROLAR RIGUROSAMENTE EL USO DE UTILIDADES QUE PUEDAN SER CAPACES DE INVALIDAR LOS CONTROLES DEL SISTEMA Y DE LA APLICACIÓN.
- SE DEBERÍA RESTRINGIR EL ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS.

# 13.REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO

PARA ALCANZAR ESTOS OBJETIVOS, ESTABLECE LOS CONTROLES:

- **RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN**
- **PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN**
- **SISTEMA DE GESTIÓN DE CONTRASEÑAS**
- **USO DE UTILIDADES CON PRIVILEGIOS DEL SISTEMA**
- **CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS**

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. **SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS**
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

PARA LA IDENTIFICACIÓN Y AUTENTICACIÓN DE UNA PERSONA FRENTE A UN SISTEMA, SE DEBE INTERCAMBIAR ALGÚN OBJETO Y/O INFORMACIÓN (**ALGO QUE SE TIENE, ALGO QUE SE SABE, O ALGO QUE SE ES).**

**ESTOS MÉTODOS PUEDEN COMBINARSE ENTRE SÍ,** INCREMENTANDO LA FORTALEZA DEL MECANISMO DE AUTENTICACIÓN, ENTENDIENDO ESTA FORTALEZA COMO UNA MEDIDA DE LOS RECURSOS QUE HABRÍA QUE DEDICAR PARA VULNERAR EL MECANISMO, ES DECIR, PARA QUE LA AUTENTICACIÓN DE LA IDENTIDAD FUERA INCORRECTA.

# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## FACTORES DE AUTENTICACIÓN

LOS MÉTODOS DE AUTENTICACIÓN SE AGRUPAN EN FACTORES DE AUTENTICACIÓN:

- **ALGO QUE SE TIENE**


- **ALGO QUE SE SABE**

- **ALGO QUE SE ES**

# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

**ALGO QUE SE TIENE**

COMO LLAVES, UN DOCUMENTO OFICIAL, UNA TARJETA IDENTIFICATIVA MAGNÉTICA, TARJETA DE RADIOFRECUENCIA, UNA TARJETA INTELIGENTE O SMARTCARD, UN ARCHIVO EN UNA UNIDAD DE ALMACENAMIENTO PORTÁTIL USB, ETC. AQUÍ SE PUEDE EMPLEAR AUTENTICACIÓN EN FUNCIÓN DE DONDE SE ESTÉ, COMO LA BASADA EN GEOLOCALIZACIÓN DE LA DIRECCIÓN IP, USO DE TERMINALES MÓVILES, Y MECANISMOS DE AUTENTICACIÓN POR MÁQUINA.

**ALGO QUE SE SABE**

DE MANERA CONFIDENCIAL SOLAMENTE COMPARTIDA CON LA ENTIDAD QUE AUTENTICA, COMO UNA CONTRASEÑA, CÓDIGO DE ACCESO, O LA RESPUESTA A UNA PREGUNTA (MÉTODO DE DESAFÍO-RESPUESTA).

# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## ALGO QUE SE ES

POR EJEMPLO, MIDIENDO CARACTERÍSTICAS FÍSICAS DE LA PERSONA (TÉCNICAS BIOMÉTRICAS) COMO SU HUELLA DACTILAR, GEOMETRÍA DE LA MANO, RECONOCIMIENTO DE LA VOZ, O PATRONES OCULARES DE IRIS O RETINA. AUNQUE PUEDEN SEPARARSE, TAMBIÉN SE SUELE INCLUIR AQUÍ LOS MÉTODOS BASADOS EN “ALGO DE QUE SE ES CAPAZ”, COMO LA CAPACIDAD DE REPRODUCIR LA FIRMA, O LA ESCRITURA CONVENIENTEMENTE PARAMETRIZADA.

# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## MÉTODOS DÉBILES Y FUERTES

UNA **AMENAZA** AL MECANISMO DE **ALGO QUE SE TIENE** ES LA **PÉRDIDA O COPIA DEL OBJETO PORTADO**.

UNA **AMENAZA** AL MECANISMO DE **ALGO QUE SE SABE** ES LA **DIVULGACIÓN DEL SECRETO COMPARTIDO.**

UNA **AMENAZA** AL MECANISMO DE **ALGO QUE SE ES** ES **UN FALSO POSITIVO**, ES DECIR, AUTENTICAR POSITIVAMENTE UNA IDENTIDAD INCORRECTA.

SI SE USAN **MECANISMOS DE AUTENTICACIÓN QUE DEBAN CUMPLIRSE SIMULTÁNEAMENTE, LA AMENAZA GLOBAL DISMINUYE** SU PROBABILIDAD, PORQUE DEBEN CONCURRIR SIMULTÁNEAMENTE LAS SITUACIONES INDIVIDUALES

# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## MÉTODOS DÉBILES Y FUERTES

UN SISTEMA DE AUTENTICACIÓN QUE SOLO EMPLEA MECANISMOS DE UN FACTOR DE AUTENTICACIÓN SUELE SER REFERIDO COMO UN MECANISMO DE **AUTENTICACIÓN DÉBIL**.

POR EL CONTRARIO, CUANDO SE EMPLEAN MECANISMOS DE VARIOS DE LOS FACTORES ANTERIORES, SE HABLA DE SISTEMAS DE AUTENTICACIÓN MULTIFACTORIALES, TAMBIÉN CONOCIDOS COMO SISTEMAS DE **AUTENTICACIÓN FUERTES**.

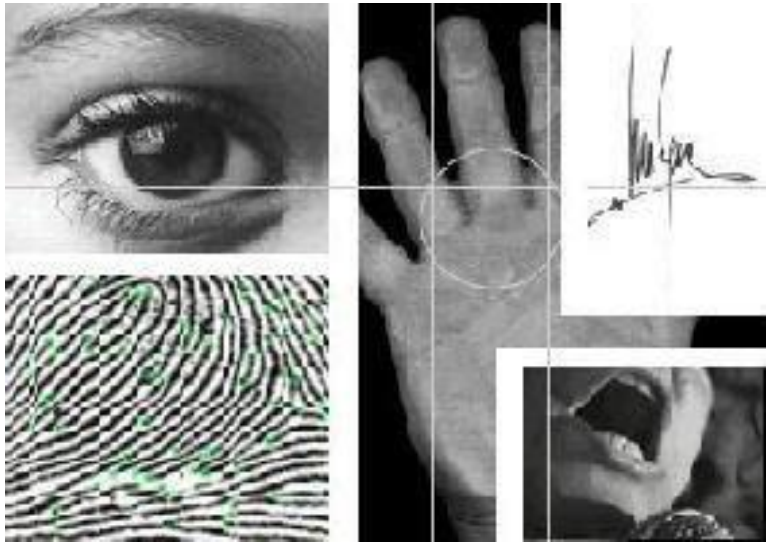
LA FORTALEZA DE UN SISTEMA DEPENDE DE LOS MECANISMOS CONCRETOS QUE SE EMPLEEN, NO SOLO DE SU TIPOLOGÍA; NO OBSTANTE, SIEMPRE QUE LOS CONTROLES DE SEGURIDAD DE USUARIO SEAN LAXOS, LA SEGURIDAD QUEDARÁ EN ENTREDICHO.

# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## MÉTODOS BIOMÉTRICOS

SE RECONOCEN COMO EL MEJOR MEDIO PARA AUTENTICAR LA IDENTIDAD DE UN SER HUMANO, PERO SUELEN CONLLEVAR UNA INVERSIÓN EN INFRAESTRUCTURA (LECTORES, CENTRALES DE SEGURIDAD, Y SERVIDOR CON APLICACIÓN DE AUTENTICACIÓN).

PERMITEN EVALUAR ALGO QUE EL USUARIO ES, O ALGO QUE EL USUARIO HACE, TOMANDO EN CONSIDERACIÓN QUE CIERTAS CARACTERÍSTICAS PUEDEN CAMBIAR.

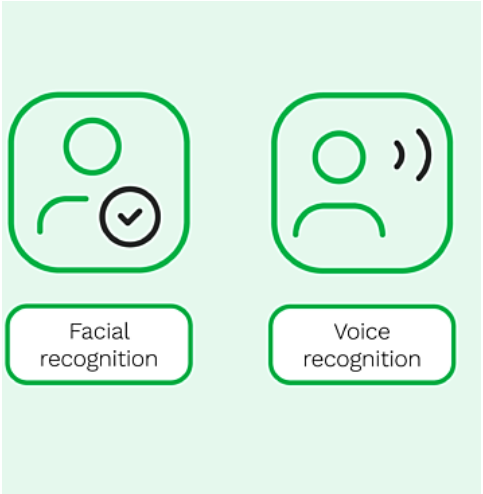


# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## MÉTODOS BIOMÉTRICOS

EL EMPLEO DE ESTOS MÉTODOS CONLLEVA UNA PRIMERA FASE, EN LA QUE SE TOMAN REITERADAS MEDIDAS QUE SE PROMEDIAN PARA DEFINIR UNA **MEDIDA PATRÓN**, QUE SERÁ LA MEDIDA BIOMÉTRICA DE REFERENCIA.

CUANDO EL USUARIO INTENTE AUTENTICARSE, SE TOMARÁN UNA O VARIAS MEDIDAS, QUE SE COMPARARÁN CON LAS MEDIDAS PATRÓN QUE EL SISTEMA TENGA REGISTRADAS, PARA DETERMINAR SI EXISTE UN ELEVADO NIVEL DE CONCORDANCIA CON ALGUNA DE ELLAS.



# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## MÉTODOS BIOMÉTRICOS

A LA HORA DE ELEGIR UN SISTEMA DE AUTENTICACIÓN BIOMÉTRICO DEBEN SER CONSIDERADOS:

- **LA TASA DE FALSOS NEGATIVOS**

  TASA DE RECHAZOS INCORRECTOS, O RECUENTO DE NO ACEPTACIONES DE LA AUTENTICACIÓN DE USUARIOS VÁLIDOS.

- **LA TASA DE FALSOS POSITIVOS**

  TASA DE ACEPTACIONES INCORRECTAS, O RECUENTO DE LAS OCASIONES EN QUE SE DA POR VÁLIDA LA AUTENTICACIÓN DE UN USUARIO INVÁLIDO.

LOS MÉTODOS BIOMÉTRICOS PUEDEN AJUSTARSE, PARA REDUCIR UN TIPO DE ERROR U OTRO, PORQUE EN GENERAL, LA REDUCCIÓN DE UNA TASA INCREMENTA LA OTRA, PRODUCIÉNDOSE UN INTERCAMBIO ENTRE PRECISIÓN AL RECHAZAR Y PRECISIÓN AL ACEPTAR.

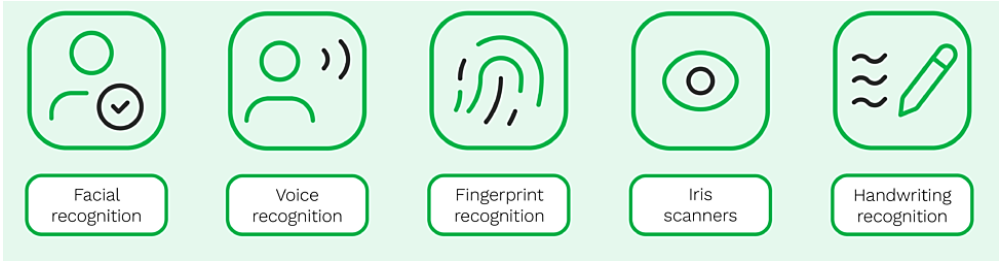
# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## MÉTODOS BIOMÉTRICOS

SE BUSCA EQUILIBRAR AMBAS TASAS, EN UN VALOR IDÉNTICO CONOCIDO COMO **TASA DE ERROR IGUAL**, QUE REPRESENTA EL PORCENTAJE DE LECTURAS DONDE SE IGUALA EL FALSO RECHAZO Y LA FALSA ACEPTACIÓN.

CUANTO MÁS BAJO SEA LA TASA DE ERROR IGUAL, MÁS EFECTIVO ES EL MECANISMO DE AUTENTICACIÓN BIOMÉTRICA.

EN GENERAL, SE OBTIENE DE MENOR A MAYOR TASA DE ERROR CON LOS SIGUIENTES INDICADORES BIOMÉTRICOS: *PALMA DE LA MANO, IRIS, RETINA, HUELLA DACTILAR, Y VOZ*.



# 14.SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS

## MEJORES PRÁCTICAS EN EL USO DE CONTRASEÑAS

LOS REQUISITOS MÍNIMOS RECOMENDADOS PARA EL USO DE CONTRASEÑAS SON:

- **DEBE SER FÁCIL DE RECORDAR PARA EL USUARIO**
- **DEBE SER DIFÍCIL DE ADIVINAR PARA UN USUARIO NO AUTORIZADO**
- **NO DEBERÍAN EMPLEARSE PALABRAS CONTENIDAS EN DICCIONARIOS**
- **NO DEBERÍAN SER INFERIORES A 8 CARACTERES**
- **UN OLVIDO DE LA CONTRASEÑA DEBE SER COMUNICADO AL ADMINISTRADOR**
- **SOLO UN ADMINISTRADOR DEBE PODER RESTABLECER LAS CONTRASEÑAS**
- **UN NÚMERO DE FALLOS DEBE BLOQUEAR LA CUENTA AUTOMÁTICAMENTE**
- **LAS CONTRASEÑAS SE DEBEN ALMACENAR Y TRANSMITIR ENCRIPTADAS**
- **LAS CONTRASEÑAS DEBEN CAMBIARSE REGULARMENTE**
- **LAS CONTRASEÑAS DEBEN SER ÚNICAS PARA UNA PERSONA**
- **LA CONTRASEÑA DEL ADMINISTRADOR DEBE SER CONOCIDA ÚNICAMENTE POR UNA PERSONA Y CUSTODIARSE DE MANERA ESPECIAL**

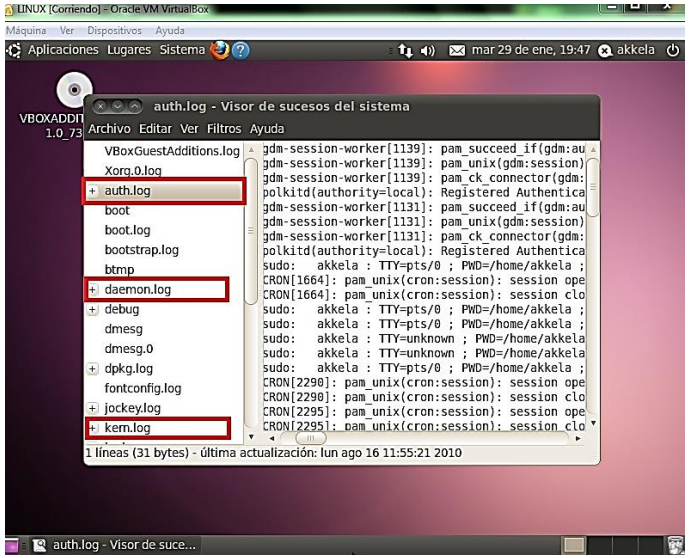
# CONTENIDOS

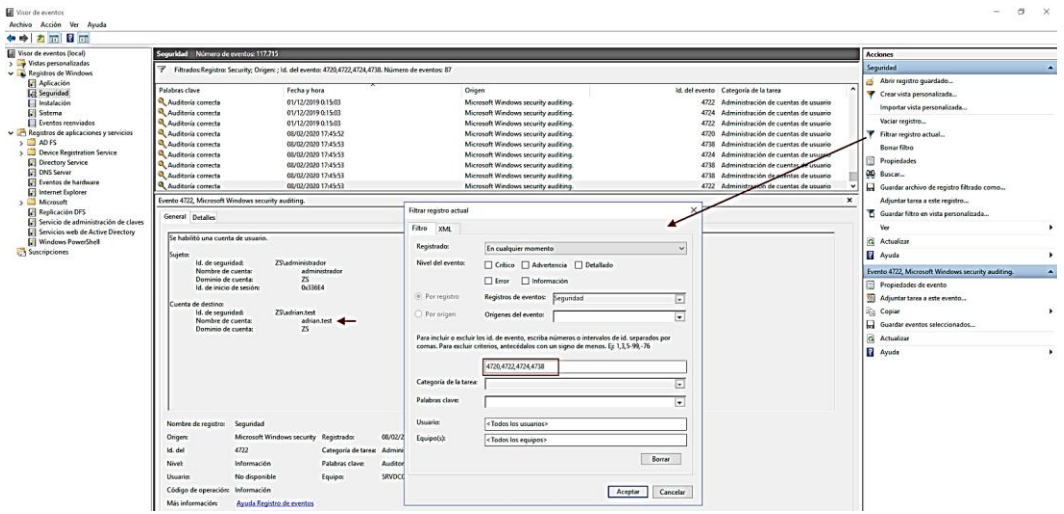
1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS**
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

# 15.RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS

PARA RECABAR EVIDENCIAS DE QUE LAS POLÍTICAS SE APLICAN, O INVESTIGAR LO CONTRARIO, **ES PRECISO REGISTRAR INFORMACIÓN** DE LO QUE HACE.

SE INTRODUCEN LAS **HERRAMIENTAS ESTÁNDAR DE REGISTRO EN SISTEMAS MICROSOFT WINDOWS Y LINUX**, PARA POSTERIORMENTE REVISAR LOS REQUISITOS QUE DICTA LA NORMA **ISO 27002**.



# 15.RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS

## REGISTRO Y MONITORIZACIÓN EN SISTEMAS WINDOWS

LOS SISTEMAS **MICROSOFT WINDOWS** INCORPORAN EL **VISOR DE SUCESOS**, QUE PERMITE FILTRAR Y CONFIGURAR LOS DIFERENTES REGISTROS.

DIVIDIDO EN CATEGORÍAS, CADA UNA SE IRÁ ESCRIBIENDO EN UN FICHERO DIFERENTE; PARA CADA UNA SE DEBE CONFIGURAR EL TAMAÑO DEL FICHERO, O EL PERIODO DE TIEMPO PARA EL QUE SE CONSERVARÁN LOS REGISTROS O LOGS.

**LA ACTIVIDAD DE REGISTRO TIENE UN COSTE** EN TÉRMINOS DE ALMACENAMIENTO, TIEMPO DE PROCESO Y POSTERIOR TIEMPO DE ANÁLISIS, POR LO QUE CONVIENE QUE VAYA PRECEDIDA DE UN ANÁLISIS DE RIESGOS, PARA FOCALIZARLO EN LAS ÁREAS Y CON EL NIVEL DE PROFUNDIDAD ADECUADO.

# 15.RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS

## REGISTRO Y MONITORIZACIÓN EN SISTEMAS WINDOWS

RESULTA CRUCIAL CONFIGURAR ADECUADAMENTE LOS EVENTOS QUE SE QUIEREN REGISTRAR.

DE ENTRE LAS CATEGORÍAS DE REGISTRO, LA CATEGORÍA DE **SEGURIDAD** REGISTRA LOS ACCESOS AL SISTEMA, Y CORRECTAMENTE CONFIGURADA, PERMITE SABER SI SE HA PRODUCIDO UN INTENTO DE ACCESO ERRÓNEO AL MISMO.

LOS SISTEMAS WINDOWS TAMBIÉN TRAEN UNA APLICACIÓN PARA **MONITORIZAR EL RENDIMIENTO DEL SISTEMA**, A TRAVÉS DE INDICADORES, COMO EL USO DE MEMORIA, DE LA RED, O DEL PROCESADOR, MEDIANTE REGISTROS DE CONTADOR.

# 15.RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS

## REGISTRO Y MONITORIZACIÓN EN SISTEMAS LINUX

LINUX EMPLEA EL SUBSISTEMA **SYSLOG** PARA TODAS LAS FUNCIONES DE REGISTRO Y MONITORIZACIÓN DE LOS EVENTOS QUE OCURREN EN EL SISTEMA, COMO EL ACCESO DE UN USUARIO.

LOS ORGANIZA EN BASE AL ORIGEN O SERVICIO QUE LOS PRODUCE (*FACILITY*) Y A SU NIVEL DE PRIORIDAD O IMPORTANCIA (*LEVEL*).

# 15.RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS

## REGISTRO Y MONITORIZACIÓN EN SISTEMAS LINUX

EN LOS ARCHIVOS DE REGISTRO DE SYSLOG, SE PODRÁN ENCONTRAR, POR EJEMPLO, ENTRADAS PROCEDENTES DE:

- AUTHPRIV: RELACIONADAS CON LA SEGURIDAD DEL SISTEMA.
- AUTH, SECURITY: RELACIONADAS CON LA AUTENTICACIÓN.
- DAEMON: PARA LOS SERVICIOS O PROCESOS QUE SE EJECUTAN EN SEGUNDO PLANO DE MANERA TRANSPARENTE AL USUARIO (DENOMINADOS “DAEMON” O DEMONIOS EN LINUX).
- USER: PARA EVENTOS DEFINIDOS POR LOS USUARIOS.
- CRON: PARA TAREAS O PROCESOS PROGRAMADOS.
- MAIL: PARA EL CORREO ELECTRÓNICO.
- FTP: PARA EL SERVIDOR DE FICHEROS
- LOCAL0...7: MENSAJES DE INICIO DE LOS TERMINALES (0..7) LOCALES.
- ETC.

# 15.RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS

## REGISTRO Y MONITORIZACIÓN EN SISTEMAS LINUX

LOS NIVELES DE IMPORTANCIA QUE HABITUALMENTE SE ENCUENTRAN SON:

- EMERG: PARA EVENTOS QUE PUEDEN INUTILIZAR EL SISTEMA.
- ALERT: PARA ERRORES QUE NECESITAN UNA ACTUACIÓN INMEDIATA.
- CRIT: PARA SITUACIONES CRÍTICAS COMO EL FALLO DE UN DISCO DURO.
- ERR: PARA ERRORES GENERALES DE LAS APLICACIONES.
- WARNING: PARA ADVERTENCIAS.
- NOTICE: PARA NOTIFICACIONES.
- INFO: PARA ANUNCIAR INFORMACIÓN DE INTERÉS.
- DEBUG: EN RELACIÓN A LA INFORMACIÓN DE DEPURACIÓN DE UNA APLICACIÓN.

# 15.RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS

## NORMA ISO 27002

EL **CAPÍTULO 12** ESTABLECE EL OBJETIVO **REGISTROS Y SUPERVISIÓN**, PARA DETECTAR LAS ACTIVIDADES NO AUTORIZADAS. SE INDICA QUE SE DEBEN REGISTRAR EVENTOS Y GENERAR EVIDENCIAS.

LA EMPRESA DEBE CONSIDERAR TAMBIÉN SU OBLIGACIÓN LEGAL A REGISTRAR ALGUNAS ACTIVIDADES, O A GUARDAR REGISTRO DE SU MONITORIZACIÓN.

# 15.RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS

## NORMA ISO 27002

ESTOS REGISTROS SERVIRÁN PARA CHEQUEAR LA EFECTIVIDAD DE LOS CONTROLES Y LA CONFORMIDAD DEL SISTEMA CON LA POLÍTICA DE ACCESO. SE DEFINEN LOS CONTROLES:

- **REGISTRO DE EVENTOS**
- **PROTECCIÓN DE LA INFORMACIÓN DEL REGISTRO**
- **REGISTROS DE ADMINISTRACIÓN Y OPERACIÓN**
- **SINCRONIZACIÓN DEL RELOJ**

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. **ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS**

# 16.ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

A LA HORA DE ELABORAR UNA NORMATIVA, SE RECOMIENDA SEGUIR UN ESQUEMA DONDE SE PRIORICEN Y SE TENGAN EN CUENTA LAS FUENTES A CONSIDERAR:

- LA LEGISLACIÓN QUE SEA DE APLICACIÓN
- LAS NORMAS DE REFERENCIA
- EL DETALLE DE LOS CONTROLES APLICADOS EN LA EMPRESA

SE EMPLEARÁ COMO REFERENCIA LA NORMA **ISO 27002**, QUE DEFINE EL CONCEPTO DE POLÍTICA DE CONTROL DE ACCESO COMO EL DOCUMENTO DE PARTIDA, QUE RECOJA LAS DIRECTRICES A PARTIR DE LAS QUE SE REDACTEN LOS DIFERENTES PROCEDIMIENTOS NECESARIOS PARA LLEVAR A CABO EL CONTROL DE ACCESO LÓGICO.

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. SISTEMAS DE CONTROL DE ACCESO FÍSICO MÁS FRECUENTES A LAS INSTALACIONES DE LA ORGANIZACIÓN Y A LAS ÁREAS EN LAS QUE ESTÉN UBICADOS LOS SISTEMAS INFORMÁTICOS
4. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS
6. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
7. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
8. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS
9. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
10. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
11. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
12. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
13. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
14. SISTEMAS DE AUTENTICACIÓN DE USUARIOS DÉBILES, FUERTES Y BIOMÉTRICOS
15. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
16. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

## RESUMEN

LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN ES ÚNICA, PERO SE ACOMETE DESDE LA PERSPECTIVA DE LA **SEGURIDAD FÍSICA (SF) Y LÓGICA (SL)**.

LA SF SE OCUPA DE LAS **BARRERAS FÍSICAS**, PROCEDIMIENTOS, Y MECANISMOS QUE SE INTERPONEN ENTRE LAS AMENAZAS FÍSICAS Y LOS ACTIVOS.

POR OTRO LADO, LA SL SE OCUPA DE LAS **BARRERAS LÓGICAS**, LOS PROCEDIMIENTOS Y MECANISMOS PARA MANTENER LOS ACTIVOS ÍNTEGROS Y A SALVO, PERMITIENDO SOLO EL ACCESO LÓGICO A LOS AGENTES AUTORIZADOS.

## RESUMEN

EN LA SF SE COMIENZA ESTUDIANDO EL **PERÍMETRO DE SEGURIDAD**, QUE PARA UNA EMPRESA PEQUEÑA O MEDIANA SE TRADUCE EN COMENZAR ASEGURANDO LAS MEDIDAS DEL CPD DONDE RESIDEN LOS SERVIDORES, MEDIOS DE ALMACENAMIENTO, Y ELECTRÓNICA CENTRAL DE COMUNICACIONES.

ES PRIMORDIAL **ASEGURAR EL SUMINISTRO ELÉCTRICO**, LOS SERVICIOS DE PROTECCIÓN CONTRA INCENDIOS Y LA CLIMATIZACIÓN; TODO ELLO SEGÚN LEYES, Y NORMAS DE DIFERENTES ÁMBITOS, COMO LA NORMA TIA 568 Y TIA 492.

## RESUMEN

EN EL ÁMBITO DE LA **SL**, SE COMIENZA ESTUDIANDO EL **SISTEMA DE FICHEROS**, DE CUYAS MEDIDAS DE SEGURIDAD DEPENDERÁ EN EL CONTROL DE ACCESO LÓGICO QUE SE LOGRE IMPLEMENTAR.

TANTO EL SISTEMA **NTFS** COMO **EXT** INCORPORAN LAS MEDIDAS NECESARIAS PARA LOS CONTROLES QUE UNA EMPRESA PEQUEÑA Y MEDIANA PRECISARÁ DESPLEGAR.

ENTRE LOS OBJETIVOS DE **CONTROL DEL ACCESO LÓGICO**, ES PRIMORDIAL QUE EL ACCESO A LA RED SOLO PUEDA REALIZARSE SOBRE UN SISTEMA ADECUADO DE IDENTIFICACIÓN Y AUTENTICACIÓN (QUE PUEDE IR DESDE EL USO DE CONTRASEÑAS HASTA EL EMPLEO DE LECTORES BIOMÉTRICOS).

## RESUMEN

A SU VEZ, LA **INFORMACIÓN DE LOS USUARIOS** SE GESTIONA MEDIANTE **DIRECTORIOS**, DONDE SE APLICAN CONFIGURACIONES Y RESTRICCIONES DE USO DEL SISTEMA.

EL **REGISTRO Y MONITORIZACIÓN DE SUCESOS** ES UNA HERRAMIENTA FUNDAMENTAL. ESTAS MEDIDAS TÉCNICAS DEBEN COMPLEMENTARSE CON LA RESPONSABILIDAD DE LOS USUARIOS, FIJADA CONTRACTUALMENTE AL INICIO, DURANTE, Y EN LA TERMINACIÓN DEL EMPLEO (Y CON SU REFLEJO EN UN PROCEDIMIENTO DE ALTAS, BAJAS Y MODIFICACIONES DE LAS CUENTAS).

## RESUMEN

EL ALCANCE DE LA **SF** Y **SL** ES MUY EXTENSO, INCLUYENDO NUMEROSAS ÁREAS TÉCNICAS. PARA ABORDARLAS CON SEGURIDAD, Y ASEGURAR QUE NADA SE QUEDA ATRÁS, SE RECOMIENDA EMPLEAR MARCOS DE TRABAJO YA EXISTENTES, COMO EL **ESQUEMA NACIONAL DE SEGURIDAD**, O LA NORMA **ISO 27000**.


ESTO ES
TODO