## IFCT0109. SEGURIDAD INFORMÁTICA

# MF0490_3 GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

# RESUMEN FINAL



DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

# CONTENIDOS

1. INTRODUCCIÓN
2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

# RESUMEN

**LA INFORMACIÓN ES UN ACTIVO MUY VALIOSO** EN CUALQUIER ORGANIZACIÓN Y MÁS EN UN MUNDO GLOBALIZADO EN EL QUE ESTA PUEDE CIRCULAR POR LOS CINCO CONTINENTES EN CUESTIÓN DE SEGUNDOS.

LA NORMA **ISO/IEC 27002** ES UNA **GUÍA DE BUENAS PRÁCTICAS** EN LA QUE SE **INCLUYE UNA SERIE DE MEDIDAS Y CONTROLES DE SEGURIDAD** QUE LAS ORGANIZACIONES

DEBEN TENER EN CUENTA PARA QUE SE ELABOREN, IMPLANTEN Y DIFUNDAN (EVALUACIÓN DE RIESGOS, SEGURIDAD EN LOS RECURSOS HUMANOS, GESTIÓN DE LOS ACTIVOS, ETC.) **ES NECESARIO ESTABLECER UN NIVEL ADECUADO DE SEGURIDAD FÍSICA** TANTO **EN LAS ÁREAS SEGURAS** DE UNA ORGANIZACIÓN **COMO EN LOS EQUIPOS** QUE FORMAN PARTE DE ELLA.

## RESUMEN

ADEMÁS DE TENER EN CUENTA LAS RECOMENDACIONES DE LA NORMATIVA **ISO/IEC 27002**, **UNA ORGANIZACIÓN DEBE SABER CÓMO PODER INTEGRAR LAS TECNOLOGÍAS DE LA INFORMACIÓN EN TODOS SUS PROCESOS**.

PARA ELLO ESTÁ LA BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN (**ITIL**), UN **CONJUNTO DE BUENAS PRÁCTICAS** QUE TIENE COMO OBJETIVO AYUDAR A ALCANZAR UNA BUENA GESTIÓN DE LOS SERVICIOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

APARTE DE UNA CORRECTA INTEGRACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LOS PROCESOS DE UNA ORGANIZACIÓN, **HAY QUE SER ESPECIALMENTE METICULOSO CON LOS DATOS DE CARÁCTER PERSONAL** QUE SE PUEDAN TRATAR, YA QUE LA PROTECCIÓN DE LOS DATOS PERSONALES **ES UN DERECHO FUNDAMENTAL** QUE TIENEN LAS PERSONAS, REFLEJADO EN LA CONSTITUCIÓN ESPAÑOLA.

# CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN
3. CARACTERÍSTICAS FUNDAMENTALES DE LOS PROCESOS ELECTRÓNICOS
4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y LOS ACTIVOS Y SERVICIOS UTILIZADOS POR LOS MISMOS
5. ANÁLISIS DE LAS FUNCIONALIDADES DE SISTEMA OPERATIVO PARA LA MONITORIZACIÓN DE LOS PROCESOS Y SERVICIOS
6. TÉCNICAS UTILIZADAS PARA LA GESTIÓN DEL CONSUMO DE RECURSOS

# RESUMEN

UN **PROCESO** ES UN **CONJUNTO DE ACTIVIDADES CONECTADAS DE MODO SISTEMÁTICO CON EL FIN DE OBTENER UN PRODUCTO O SERVICIO QUE TENGA VALOR PARA EL CLIENTE**.

MÁS CONCRETAMENTE, UN **PROCESO DE NEGOCIO** CONSISTE EN EL **CONJUNTO DE TAREAS O ACTIVIDADES QUE SE LLEVAN A CABO DE UN MODO LÓGICO PARA CONSEGUIR UN NEGOCIO DEFINIDO, AÑADIENDO VALOR AL PRODUCTO O SERVICIO FINAL**.

SE DISTINGUE ENTRE PROCESOS **ESTRATÉGICOS, SUSTANTIVOS, DE APOYO VERTICAL Y DE APOYO HORIZONTAL**.

# RESUMEN

**LAS ORGANIZACIONES SON TAN EFICIENTES COMO SUS PROCESOS**, POR ELLO ES FUNDAMENTAL PLANIFICAR Y LLEVAR A CABO UNA GESTIÓN EFICIENTE DE LOS PROCESOS, INTEGRANDO EN LA ORGANIZACIÓN LOS SISTEMAS DE INFORMACIÓN.

POR ELLO, LOS DATOS DE LAS EMPRESAS HAN PASADO A SER UNA FUENTE DE INFORMACIÓN BÁSICA **Y ES NECESARIO LLEVAR A CABO TAREAS DE RECOLECCIÓN, ANÁLISIS Y PROCESAMIENTO DE DATOS DE UN MODO AUTOMATIZADO A TRAVÉS DE PROCESOS ELECTRÓNICOS**.

**UN PROCESO ELECTRÓNICO** CONSISTE EN **CUALQUIER PROGRAMA EN EJECUCIÓN Y NECESITA UNA SERIE DE RECURSOS** (TIEMPO DE CPU, MEMORIA, ARCHIVOS, ETC.) **PARA REALIZAR SU TAREA CON ÉXITO**.

# RESUMEN

TANTO LOS PROCESOS ELECTRÓNICOS COMO LOS RECURSOS QUE SE UTILIZAN DEBEN TENER UN RENDIMIENTO ÓPTIMO, Y PARA CONSEGUIRLO **HAY UNA SERIE DE HERRAMIENTAS EN LOS SISTEMAS OPERATIVOS** CUYAS FUNCIONALIDADES PRINCIPALES SON EL **CONTROL Y LA GESTIÓN DE LOS PROCESOS, RECURSOS Y RENDIMIENTOS**, PARA QUE SE REDUZCA LA LATENCIA Y AUMENTE EL RENDIMIENTO, LA UTILIZACIÓN Y LA EFICIENCIA DE LOS SISTEMAS OPERATIVOS.

ADEMÁS DE ESTABLECER SISTEMAS PREVENTIVOS DE DETECCIÓN DE POSIBLES ERRORES, **LOS ADMINISTRADORES DEBEN** SABER QUÉ PASOS SEGUIR PARA **RESPONDER CON EFICACIA Y EFICIENCIA ANTE LOS FALLOS SUCEDIDOS** Y PODER VOLVER A LA SITUACIÓN DE PARTIDA PREVIA A LA INCIDENCIA, SIGUIENDO UNOS PROCESOS DE DIAGNÓSTICO, DETECCIÓN Y RESOLUCIÓN DE INCIDENCIAS.

# CONTENIDOS

1. INTRODUCCIÓN
2. TIPOS DE DISPOSITIVOS DE ALMACENAMIENTO MÁS FRECUENTES
3. CARACTERÍSTICAS DE LOS SISTEMAS DE ARCHIVO DISPONIBLES
4. ORGANIZACIÓN Y ESTRUCTURA GENERAL DE ALMACENAMIENTO
5. HERRAMIENTAS DEL SISTEMA PARA LA GESTIÓN DE DISPOSITIVOS DE ALMACENAMIENTO

# RESUMEN

HOY EN DÍA, **SE MANEJA UNA GRAN CANTIDAD DE INFORMACIÓN**. PARA ALMACENARLA **SE UTILIZAN** DISTINTOS **DISPOSITIVOS**, DEFINIDOS COMO COMPONENTES QUE LEEN O ESCRIBEN DATOS EN MEDIOS O SOPORTES **DE ALMACENAMIENTO**.

HAY GRAN VARIEDAD DE DISPOSITIVOS DE ALMACENAMIENTO Y LA ELECCIÓN DEL IDÓNEO DEPENDE DE **FACTORES** COMO LA **FINALIDAD** DE LA INFORMACIÓN UTILIZADA, EL **TAMAÑO** DE DICHA INFORMACIÓN Y EL **RENDIMIENTO** QUE SE PRETENDE OBTENER DEL DISPOSITIVO.

EL **SISTEMA DE ARCHIVOS O FILESYSTEM ES LA FORMA EN LA QUE EL SISTEMA OPERATIVO ORGANIZA LA INFORMACIÓN DENTRO DE UN DISPOSITIVO** DE ALMACENAMIENTO PARA SU GRABACIÓN Y POSTERIOR RECUPERACIÓN.

# RESUMEN

**LOS SISTEMAS DE ARCHIVOS SE CARACTERIZAN POR LA CAPACIDAD DE ABSTRACCIÓN** Y DE **UTILIZAR ENLACES DUROS Y SIMBÓLICOS** Y POR LA POSIBILIDAD DE **ASIGNAR PERMISOS DE UTILIZACIÓN** DE LOS ARCHIVOS, PERMITIENDO O DENEGANDO SU ACCESO A LOS USUARIOS.

LA CORRECTA **ELECCIÓN DEL SISTEMA ADECUADO DEPENDERÁ** SOBRE TODO **DEL SISTEMA OPERATIVO** QUE SE VA A UTILIZAR **Y** DE **OTRAS CARACTERÍSTICAS** *COMO* ***EL NÚMERO MÁXIMO DE ARCHIVOS*** *QUE SE PUEDEN ALMACENAR, EL* ***TAMAÑO MÁXIMO DE VOLUMEN*** *Y LA* ***CAPACIDAD DE JOURNALING****.*

**LOS DATOS SE GUARDAN EN** LOS DISPOSITIVOS DE ALMACENAMIENTO MEDIANTE UNA SERIE DE ESTRUCTURAS LLAMADAS **ARCHIVOS O FICHEROS** (CONSTITUIDOS POR REGISTROS QUE A SU VEZ ESTÁN FORMADOS POR CAMPOS).

# RESUMEN

**LA ORGANIZACIÓN DE UN ARCHIVO DEFINE LA FORMA EN LA QUE LOS REGISTROS SE DISPONEN** SOBRE EL SOPORTE DE ALMACENAMIENTO, DISTINGUIÉNDOSE CINCO TIPOS DE ORGANIZACIONES**: PILA, SECUENCIAL, DIRECTA, INDEXADA Y SECUENCIAL INDEXADA**.

**PARA GESTIONAR LOS DISPOSITIVOS DE ALMACENAMIENTO, SUS SISTEMAS DE ARCHIVO Y LOS ARCHIVOS** QUE CONTIENEN HAY UNA SERIE DE **HERRAMIENTAS** DISPONIBLES DIRECTAMENTE EN CADA SISTEMA OPERATIVO (EN WINDOWS ESTÁ EL **ADMINISTRADOR DE DISCOS** Y EN LINUX, **GPARTED**).

# CONTENIDOS

1. INTRODUCCIÓN
2. CRITERIOS PARA ESTABLECER EL MARCO GENERAL DE USO DE MÉTRICAS E INDICADORES PARA LA MONITORIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN
3. IDENTIFICACIÓN DE LOS OBJETOS PARA LOS CUALES ES NECESARIO OBTENER INDICADORES
4. ASPECTOS A DEFINIR PARA LA SELECCIÓN Y DEFINICIÓN DE INDICADORES
5. ESTABLECIMIENTO DE LOS UMBRALES DE RENDIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
6. RECOLECCIÓN Y ANÁLISIS DE LOS DATOS APORTADOS POR LOS INDICADORES
7. CONSOLIDACIÓN DE INDICADORES BAJO UN CUADRO DE MANDO DE RENDIMIENTO DE SISTEMAS DE INFORMACIÓN UNIFICADO

# RESUMEN

HOY EN DÍA, **LOS SISTEMAS DE INFORMACIÓN SUMINISTRAN UNA ELEVADA CANTIDAD DE DATOS** MUY DETALLADOS Y PUEDE RESULTAR DIFICULTOSO SABER CUÁLES DE ESTOS DATOS SON RELEVANTES Y CUÁLES HAY QUE DESECHAR.

POR ELLO, **ES NECESARIO** TOMAR UNA SERIE DE DECISIONES Y MEDICIONES DE LOS DATOS RELEVANTES PARA **SABER CUÁLES SON LOS OBJETIVOS** QUE DEBE CUMPLIR LA ORGANIZACIÓN **Y QUÉ DATOS** SON LOS QUE **VAN A REFLEJAR LA EVOLUCIÓN EN LA CONSECUCIÓN DE ESTOS OBJETIVOS**.

**LAS MÉTRICAS** SON LAS UNIDADES DE MEDIDA QUE SE UTILIZAN COMO REFERENCIA PARA ENTENDER LOS DATOS Y TOMAR RELACIONES AL RESPECTO.

# RESUMEN

SIN EMBARGO, LOS **INDICADORES** SON LOS PROCEDIMIENTOS QUE CUANTIFICAN Y FACILITAN INFORMACIÓN SOBRE EL ESTADO GENERAL DE UN ATRIBUTO DE LA ORGANIZACIÓN QUE SE QUIERA MEDIR.

HAY UNA **GRAN VARIEDAD DE MÉTRICAS E INDICADORES**, Y LA SELECCIÓN DE LA TIPOLOGÍA DE CADA UNO DE ELLOS **DEPENDERÁ DE LOS OBJETIVOS DE CADA ORGANIZACIÓN.**

**UNA ELECCIÓN CORRECTA ES LO QUE PUEDE MARCAR LA DIFERENCIA ENTRE EL ÉXITO Y EL FRACASO DE UNA ORGANIZACIÓN.**

# RESUMEN

**PARA UNA CORRECTA ELECCIÓN Y DEFINICIÓN** DE LAS MÉTRICAS E INDICADORES **HAY QUE SEGUIR METÓDICAMENTE UNA SERIE DE FASES**.

SIGUIÉNDOLAS **SE CONSIGUE IDENTIFICAR Y ESTABLECER LOS OBJETIVOS Y LAS METAS** QUE DEBEN ESTAR **RELACIONADOS CON CADA INDICADOR**, IDENTIFICAR LAS DISTINTAS CARACTERÍSTICAS DE CADA UNO DE LOS INDICADORES Y LOS UMBRALES Y VALORES IDEALES, ACEPTABLES Y CRÍTICOS QUE DEBEN TOMAR Y CÓMO ANALIZAR LOS DATOS QUE PROPORCIONAN CORRECTAMENTE.

UNA VEZ VALIDADOS LOS INDICADORES Y OBTENIDOS LOS RESULTADOS HAY QUE **REFLEJARLOS Y REPRESENTARLOS EN UN INFORME** QUE SIRVA PARA QUE EL DESTINATARIO PUEDA **OBTENER UNA VISIÓN GLOBAL DE LOS INDICADORES Y PUNTOS CLAVE DE LA ORGANIZACIÓN**, **Y** PUEDA **TOMAR LAS DECISIONES** CON MAYOR FACILIDAD Y PROBABILIDAD DE ÉXITO.

# CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

# RESUMEN

UNA **RED** ES UN **CONJUNTO DE DISPOSITIVOS FÍSICOS Y DE APLICACIONES MEDIANTE EL CUAL SE COMUNICAN LOS ORDENADORES PARA COMPARTIR INFORMACIÓN Y ESTABLECER UN SISTEMA DE COMUNICACIÓN EN UNA ORGANIZACIÓN**.

SON VARIOS LOS DISPOSITIVOS QUE FORMAN PARTE DE UNA RED, DISTINGUIENDO ENTRE **EQUIPOS DE RED** (*SERVIDORES, ORDENADORES*), **MEDIOS DE COMUNICACIÓN** (ROUTERS, SWITCHES...) **Y CONECTORES** (SISTEMA DE CABLEADO, ENLACES INALÁMBRICOS...).

PARA QUE LOS DISTINTOS EQUIPOS DE RED SE COMUNIQUEN ENTRE ELLOS Y PUEDAN TRANSMITIR LA INFORMACIÓN **ES NECESARIO EL ESTABLECIMIENTO DE UNA SERIE DE NORMAS Y REGLAS**: ESTE CONJUNTO DE NORMAS Y REGLAS FORMAN EL **PROTOCOLO**.

# RESUMEN

LA VARIEDAD DE PROTOCOLOS ES MUY AMPLIA Y TIENEN BASTANTES DIFERENCIAS ENTRE ELLOS, AUNQUE LO HABITUAL ES QUE COMPARTAN ALGUNA PROPIEDAD FUNDAMENTAL.

**EL PRIMER PASO PARA LA ESTANDARIZACIÓN** DE LOS PROTOCOLOS **FUE** CON **EL MODELO OSI** (OPEN SYSTEM INTERCONNECTION), UN **MODELO TEÓRICO** QUE EN LA ACTUALIDAD FORMA UN **MARCO DE REFERENCIA** PARA LA DEFINICIÓN DE ARQUITECTURA EN LA INTERCONEXIÓN DE LOS SISTEMAS DE COMUNICACIONES.

NO OBSTANTE, EN LA PRÁCTICA SE UTILIZA **EL MODELO TCP/IP** PARA LA DESCRIPCIÓN DE PROTOCOLOS DE RED.

# RESUMEN

**PARA TENER UN CONTROL** DE LOS DISTINTOS PARÁMETROS DE UN SISTEMA DE COMUNICACIONES **ES NECESARIO SU MONITORIZACIÓN**, PARA OBTENER **DATOS DE RENDIMIENTO** DE LOS DISTINTOS COMPONENTES DE LA RED, **REALIZAR UN ANÁLISIS** DE LOS MISMOS **Y TOMAR DECISIONES** PARA SEGUIR CON LA ESTRATEGIA DE RED DEFINIDA O, POR EL CONTRARIO, REALIZAR MODIFICACIONES EN CASO DE SER NECESARIO.

EN RESUMEN, ES IMPRESCINDIBLE **REMARCAR LA IMPORTANCIA DE LA SEGURIDAD DE LOS SISTEMAS DE COMUNICACIÓN.**

POR ELLO, HAY **SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** (**SIM**), **SISTEMAS DE GESTIÓN DE EVENTOS** (**SEM**) Y **SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD** (**SIEM**).

# CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DEL NIVEL DE REGISTROS NECESARIO, LOS PERIODOS DE RETENCIÓN Y LAS NECESIDADES DE ALMACENAMIENTO
3. ANÁLISIS DE LOS REQUERIMIENTOS LEGALES EN REFERENCIA AL REGISTRO
4. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DEL SISTEMA DE REGISTROS
5. ASIGNACIÓN DE RESPONSABILIDADES PARA LA GESTIÓN DEL REGISTRO
6. ALTERNATIVAS DE ALMACENAMIENTO PARA LOS REGISTROS DEL SISTEMA Y SUS CARACTERÍSTICAS DE RENDIMIENTO, ESCALABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD
7. GUÍA PARA LA SELECCIÓN DEL SISTEMA DE ALMACENAMIENTO Y CUSTODIA DE REGISTROS

# RESUMEN

LOS PROCESOS DE MONITORIZACIÓN DE SISTEMAS DE INFORMACIÓN OFRECEN UNA SERIE DE DOCUMENTOS QUE SON DE UTILIDAD PARA LOS DIRECTIVOS EN EL MOMENTO DE LA TOMA DE DECISIONES.

LOS **REGISTROS** SON **FORMATOS O IMPRESOS CUMPLIMENTADOS COMO RESULTADO DE LA REALIZACIÓN DE UNA TAREA** DE UN SISTEMA DE LA ORGANIZACIÓN.

**TODAS LAS TAREAS** QUE REALICE UNA ORGANIZACIÓN Q**UEDARÁN DOCUMENTADAS EN UN REGISTRO,** QUE DEBE CUMPLIR CON UNA SERIE DE **PROPIEDADES**: **IDENTIFICACIÓN, ALMACENAMIENTO, PROTECCIÓN, RECUPERACIÓN, RETENCIÓN Y DISPOSICIÓN**.

# RESUMEN

**EL ALMACENAMIENTO DE REGISTROS ESPECIALES** PUEDE SUPONER A LA ORGANIZACIÓN LA OBLIGACIÓN DEL **CUMPLIMIENTO DE UNAS CONDICIONES LEGALES** REFLEJADAS EN LAS DISTINTAS **NORMATIVAS VIGENTES**, LA MÁS IMPORTANTE **LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTÍA DE LOS DERECHOS DIGITALES.**

EL CUMPLIMIENTO DE ESTOS REQUERIMIENTOS LEGALES SERÁ UNA DE LAS MEDIDAS DE UN PLAN DE SEGURIDAD DE LA ORGANIZACIÓN, PERO NO LA ÚNICA.

EN EL **DOCUMENTO DE SEGURIDAD** TAMBIÉN **ES NECESARIO EL ESTABLECIMIENTO DE UNA SERIE DE MEDIDAS QUE AUMENTEN LA SEGURIDAD DEL SISTEMA DE REGISTROS**, ACORDES CON SU VALOR Y CON EL DAÑO QUE SE PUEDE OCASIONAR EN CASO DE SU PÉRDIDA.

ESTAS **MEDIDAS DE SEGURIDAD PUEDEN SER ADMINISTRATIVAS, FÍSICAS O TÉCNICAS**.

# RESUMEN

**LAS ORGANIZACIONES DEBEN ASIGNAR RESPONSABLES** QUE SE ENCARGUEN DE GARANTIZAR LOS REQUERIMIENTOS LEGALES Y DE SEGURIDAD ESTABLECIDOS.

**LOS REGISTROS HAY QUE ALMACENARLOS** DE MODO QUE **SE GARANTICE EL RENDIMIENTO, ESCALABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DEL SISTEMA.** LAS ALTERNATIVAS DE ALMACENAMIENTO DEL REGISTRO PUEDEN SER DISTINTAS: MIENTRAS QUE EN **WINDOWS** SE PUEDE UTILIZAR UNA APLICACIÓN PARA GESTIONAR LOS REGISTROS, EN **LINUX** ES NECESARIA LA UTILIZACIÓN DE COMANDOS.

ADEMÁS, **LA ELECCIÓN DEL SISTEMA DE ALMACENAMIENTO Y CUSTODIA DE ESTOS REGISTROS DEBE REALIZARSE TENIENDO EN CUENTA LAS CARACTERÍSTICAS DE LA ORGANIZACIÓN Y DE LOS REGISTROS**.

# CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

# RESUMEN

ES FUNDAMENTAL **REALIZAR UN ANÁLISIS INICIAL DE LOS REQUERIMIENTOS DE ACCESO** EN EL MOMENTO DE **DEFINIR LA POLÍTICA DE ACCESO DE LOS SISTEMAS DE INFORMACIÓN** DE UNA ORGANIZACIÓN.

ESTOS REQUERIMIENTOS SE ENCUENTRAN RECOGIDOS PRINCIPALMENTE EN LA NORMATIVA **ISO/IEC 27002** Y, CONCRETAMENTE, EN EL **APARTADO 9**.

ADEMÁS DE LA NORMATIVA MENCIONADA, TAMBIÉN HAY QUE REFERIRSE AL **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS UE 679/2016**, QUE HACE MENCIÓN A LAS **MEDIDAS** QUE DEBEN TOMAR LAS ORGANIZACIONES **DEPENDIENDO DEL NIVEL DE SEGURIDAD DE LOS DATOS**: **BÁSICO, MEDIO O ALTO**. A MAYOR NIVEL DE SEGURIDAD, MAYORES DEBEN SER LAS MEDIDAS A TOMAR.

# RESUMEN

UNA VEZ DEFINIDA LA POLÍTICA DE SEGURIDAD DE LA EMPRESA Y REVISADAS LAS MEDIDAS DE SEGURIDAD QUE HAY QUE TOMAR, ATENDIENDO A LOS REQUERIMIENTOS LEGALES ESTABLECIDOS, YA SE PUEDEN **DEFINIR LOS DISTINTOS PERFILES DE ACCESO DE LA ORGANIZACIÓN** ATENDIENDO AL PUESTO DE TRABAJO QUE OCUPAN DENTRO DE ELLA.

NO TODOS LOS EMPLEADOS DEBEN PODER ACCEDER Y UTILIZAR EL MISMO TIPO DE INFORMACIÓN, TODO LO CONTRARIO: SERÁ VITAL OBSERVAR EL **ORGANIGRAMA DE LA ORGANIZACIÓN Y LAS FUNCIONALIDADES Y RESPONSABILIDADES** DE CADA PUESTO DE TRABAJO PARA ASÍ ASIGNARLES ACCESO Y PRIVILEGIOS EXCLUSIVAMENTE A LA INFORMACIÓN NECESARIA Y PERTINENTE PARA CADA EMPLEADO.

# RESUMEN

HAY VARIAS **HERRAMIENTAS DE CONTROL DE ACCESOS**:

- **LAS HERRAMIENTAS DE DIRECTORIO ACTIVO** GESTIONAN TODOS LOS ELEMENTOS QUE FORMAN PARTE DE UNA RED
- **LAS HERRAMIENTAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES** (**IAM**) GESTIONAN LA IDENTIDAD DE LAS PERSONAS QUE ACCEDEN A LOS RECURSOS DEL SISTEMA DE INFORMACIÓN Y QUE PUEDE HACER CADA USUARIO CON ESTOS.
- LAS **HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN O SINGLE SIGN ON (SSO)**, QUE FACILITAN QUE LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN SOLO TENGAN QUE IDENTIFICARSE UNA VEZ PARA ACCEDER A LOS DISTINTOS SERVICIOS DEL SISTEMA DE INFORMACIÓN.

CON TODAS ESTAS HERRAMIENTAS, LAS ORGANIZACIONES PUEDEN LLEVAR A CABO **UNA POLÍTICA DE CONTROL DE ACCESOS ACTIVA Y EFICIENTE Y AUMENTAR ASÍ EL NIVEL DE SEGURIDAD DE LA ORGANIZACIÓN**.

# ACTIVIDADES

- ACTIVIDAD 01. ELABORACIÓN DE GLOSARIO DE TÉRMINOS
- ACTIVIDAD 02. INSTALACIÓN DE VIRTUALBOX
- ACTIVIDAD 03. COMANDOS BÁSICOS DE LINUX
- ACTIVIDAD 04. CONTROLES ISO 27002
- ACTIVIDAD 05. SISTEMAS DE NUMERACIÓN DECIMAL, BINARIO, OCTAL Y DECIMAL
- ACTIVIDAD 06. SURFACE WEB, DEEP WEB, DARK WEB Y DARKNET
- ACTIVIDAD 07. CARPETAS PRINCIPALES DE LOS SISTEMAS OPERATIVOS WINDOWS Y LINUX (E1)
- ACTIVIDAD 08. PRÁCTICAS DE GESTIÓN ITIL
- ACTIVIDAD 09. COMANDOS BÁSICOS CMD DE WINDOWS

# ACTIVIDADES

- ACTIVIDAD 10. CONTROL DE PROCESOS EN LINUX Y WINDOWS
- ACTIVIDAD 11. USO AVANZADO DE VIRTUALBOX
- ACTIVIDAD 12. CREAR UNIDADES DE DISCO (E2)
- ACTIVIDAD 13. HERRAMIENTAS DE GESTIÓN DE PARTICIONES
- ACTIVIDAD 14. SISTEMAS DE ARCHIVOS
- ACTIVIDAD 15. EL REGISTRO DE WINDOWS
- ACTIVIDAD 16. CREAR RAID 5 LINUX (E3)
- ACTIVIDAD 17. INSTALACIÓN DE SERVIDOR SAMBA EN LINUX

# ANEXOS

- ISO 27000
- CARPETAS PRINCIPALES DE LOS SISTEMAS OPERATIVOS WINDOWS Y LINUX
- MF0490-DESCRIPCIÓN DE LOS CONCEPTOS BÁSICOS DE LA CIBERSEGURIDAD
- MF0490-INTRODUCCIÓN A LA TECNOLOGÍA
- ITIL
- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
- EL DIRECCIONAMIENTO IP
- PARTICIONES
- COPIAS DE SEGURIDAD
- EL REGISTRO DE WINDOWS
- CREAR RAID 5 LINUX
- CREAR UN RAID DISTRIBUIDO CON PARIDAD EN WINDOWS
- GESTIÓN DE USUARIOS EN WINDOWS Y LINUX

# ESTO ES TODO