## IFCT0109. SEGURIDAD INFORMÁTICA

# MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

# UD08

## ROBUSTECIMIENTO DE SISTEMAS



DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

# 1. INTRODUCCIÓN

REDUCIR LA VULNERABILIDAD DE UN SISTEMA, LO QUE TAMBIÉN SE CONOCE COMO **ROBUSTECIMIENTO, SECURIZACIÓN DE SISTEMAS O HARDENING,** PERMITE POR LO TANTO REDUCIR EL RIESGO DE UNA AMENAZA, APLICÁNDOSE CASI EN EXCLUSIVIDAD **A LA SEGURIDAD LÓGICA** DEL SISTEMA.

# 1. INTRODUCCIÓN

**REDUCIR LAS VULNERABILIDADES DE UN SISTEMA ES UNA TAREA ESPECÍFICA Y EN OCASIONES ALTAMENTE ESPECIALIZADA.**

DEPENDERÁ DE LA FUNCIÓN, SERVICIO, PROTOCOLO, O APLICACIÓN CONCRETA QUE CORRA EN EL SISTEMA, LO QUE SIN DUDA **REQUIERE CONOCERLA, AL MENOS TAN EXHAUSTIVAMENTE COMO EL ATACANTE**.

DEBE APLICARSE EL **PRINCIPIO DE PROPORCIONALIDAD**, QUE DICTA QUE EL ESFUERZO EN ROBUSTECER UN SISTEMA SE COMPARE CON EL DEL VALOR DEL SISTEMA PROTEGIDO.

# 1. INTRODUCCIÓN

**EL ROBUSTECIMIENTO** PUEDE VALORARSE COMO **UNA CONTRAMEDIDA** CON UN COSTE Y REDUCCIÓN DE RIESGO, A COMPARAR FRENTE A OTRAS SALVAGUARDAS. SE DAN 3 **DIRECTRICES BÁSICAS A CUMPLIR:**

- EL ROBUSTECIMIENTO PARTE COMO PREMISA DE **MINIMIZAR LA SUPERFICIE DE UN ATAQUE LÓGICO**, ACEPTÁNDOSE QUE *LA SUPERFICIE DE ATAQUE ES MAYOR CUANTAS MÁS FUNCIONES DESEMPEÑE EL SISTEMA*. ASÍ, **UN SISTEMA QUE SOLO DESEMPEÑA UNA FUNCIÓN ES**, A PRIORI, **MENOS VULNERABLE QUE UN SISTEMA MULTIFUNCIÓN**.
- ADEMÁS DE **REDUCIR QUÉ HACE EL SISTEMA Y QUIÉN LO HACE** , *ELIMINANDO APLICACIONES, SERVICIOS Y USUARIOS INNECESARIOS*.
- **ESTE PROCESO EXIGE UNA REVISIÓN CONTINUA**, A LA VEZ QUE SE CONOCEN, DESCUBREN, Y EXPLOTAN NUEVAS VULNERABILIDADES EN LAS APLICACIONES QUE CORRA EL SISTEMA.

# CONTENIDOS

1. INTRODUCCIÓN
2. **MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN**
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## 2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN

LOS **SISTEMAS OPERATIVOS**, **Y** MUCHAS OTRAS **APLICACIONES**, **EMPLEAN** EL CONCEPTO DE **CUENTAS DE USUARIO**, PARA FORMAR UN SISTEMA DE CONTROL DE ACCESO LÓGICO, QUE PERSIGUE QUE SOLO LOS USUARIOS AUTORIZADOS TENGAN ACCESO A LA INFORMACIÓN.

SI LOS SISTEMAS OPERATIVOS Y LAS APLICACIONES **INCORPORAN CUENTAS DE USUARIO, Y CONTRASEÑAS CREADAS POR EL FABRICANTE Y PÚBLICAMENTE CONOCIDAS**.

EL CONTROL DE **ACCESO LÓGICO** A ESOS **PRODUCTOS NO ES EFICAZ, HASTA MODIFICAR LAS CONTRASEÑAS** PARA RECUPERAR SU CONFIDENCIALIDAD.

# 2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN

## USUARIOS Y CONTRASEÑAS POR DEFECTO

LAS **CLAVES SECRETAS PREDETERMINADAS** POR EL FABRICANTE SIEMPRE **DEBEN SER CAMBIADAS** TRAS INSTALAR EL EQUIPO O LA APLICACIÓN.

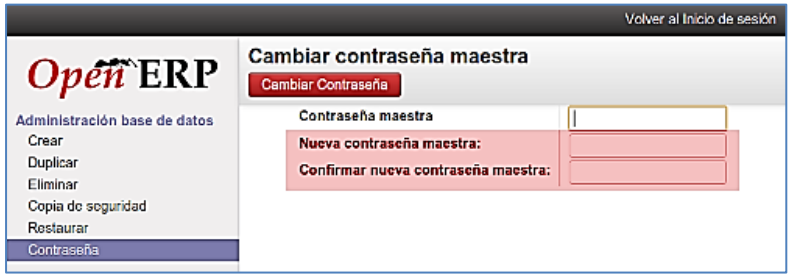
ESTO RESULTA ESPECIALMENTE CRÍTICO, PORQUE **LOS USUARIOS CREADOS POR EL FABRICANTE NORMALMENTE DISPONEN DE PRIVILEGIOS PARA LA CONFIGURACIÓN O PARAMETRIZACIÓN DEL SISTEMA. LA OMISIÓN DE ESTA MEDIDA PRIMORDIAL INUTILIZA TODO EL CONTROL DE ACCESO LÓGICO AL SISTEMA.**

# 2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN

## USUARIOS Y CONTRASEÑAS POR DEFECTO

**SIEMPRE QUE SEA POSIBLE, DEBEN DESHABILITARSE LOS USUARIOS QUE EL SISTEMA INCORPORA POR DEFECTO. EL ACCESO LÓGICO PRECISA UN USUARIO Y SU CONTRASEÑA**, DE MANERA QUE CONOCER UN NOMBRE DE USUARIO VÁLIDO, YA **ES UNA DEBILIDAD DEL SISTEMA**.

SE DEBE **REVISAR LA DOCUMENTACIÓN DEL SISTEMA PARA CAMBIAR LAS CREDENCIALES POR DEFECTO** Y CONTRASTAR QUE EL SISTEMA PUEDA OPERAR SIN USUARIOS HABILITADOS POR DEFECTO, Y QUE **NO EXISTAN CONTRASEÑAS MAESTRAS** ADICIONALES.



# 2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN

## USUARIOS Y CONTRASEÑAS POR DEFECTO

DEBE APLICARSE **ESPECIAL PRECAUCIÓN EN LOS MECANISMOS QUE PERMITAN RETORNAR EL EQUIPO A SU ESTADO DE FÁBRICA** Y VOLVER A HABILITAR Y RESTABLECER LAS CONTRASEÑAS POR DEFECTO DE UN SISTEMA. **CONSTITUYE UNA IMPORTANTE VULNERABILIDAD**.


EN EQUIPOS FÍSICOS, SUELE SER HABITUAL LA EXISTENCIA DE ALGÚN PULSADOR, QUE PERMITE CARGAR LA CONFIGURACIÓN CON LA QUE EL FABRICANTE ENTREGÓ EL EQUIPO. **EN ESTE CASO, DEBEN APLICARSE LAS MEDIDAS DE CONTROL DE ACCESO FÍSICO**.

# 2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN

## USUARIOS Y CONTRASEÑAS POR DEFECTO

TAMBIÉN **SUELE SER POSIBLE DEVOLVER UN EQUIPO,** O UNA APLICACIÓN, **A SU ESTADO ORIGINAL, MEDIANTE LA EJECUCIÓN DE ALGÚN COMANDO DE RESTABLECIMIENTO,** CUYA EJECUCIÓN HAY QUE ASEGURAR QUE **SOLO SEA POSIBLE PARA USUARIOS CON PRIVILEGIOS**.

EN SISTEMAS OPERATIVOS **LINUX**, LA CUENTA DE MÁXIMOS PERMISOS ES LA CUENTA **ROOT** O DE **SUPERUSUARIO**, Y EN SISTEMAS OPERATIVOS **WINDOWS**, ES **ADMINISTRADOR**.

**NO SE DEBE EMPLEAR PARA INICIAR SESIÓN DE MANERA REGULAR**, SIENDO PREFERIBLE EMPLEAR OTRAS CUENTAS PARA LOS TRABAJOS DE ADMINISTRACIÓN.

# 2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN

## USUARIOS Y CONTRASEÑAS POR DEFECTO

DEBE TENERSE EN CUENTA QUE **EL SISTEMA PUEDE ADMITIR UN MODO DE ARRANQUE A PRUEBA DE FALLOS O ARRANQUE SEGURO**, ORIENTADO A LA RECUPERACIÓN DEL SISTEMA, EN EL CUAL PUEDE QUE ESTAS CUENTAS SE HABILITEN AUTOMÁTICAMENTE, O INCLUSO SE PRODUZCA UN INICIO DE SESIÓN AUTOMÁTICO.

ADEMÁS, **DEBEN REVISARSE**: LAS **CUENTAS DE INVITADO** (*GUEST*), LAS **CUENTAS DE ACCESO ANÓNIMO** (*ANONYMOUS*) SI LAS HUBIERA, QUE, AUNQUE CON MENOS PRIVILEGIOS, PUEDEN USARSE PARA GANAR ACCESO AL SISTEMA

# 2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN

## USUARIOS Y CONTRASEÑAS POR DEFECTO

TAMBIÉN **LAS CUENTAS QUE NO NECESITAN INICIAR SESIÓN DE MANERA INTERACTIVA DEBEN DESHABILITARSE O RESTRINGIRSE** A LOS PROCESOS, SERVICIOS, Y FICHEROS QUE NECESITEN EXCLUSIVAMENTE.

EN CASO DE QUE NO SE PUEDA DESHABILITAR LA CUENTA DE ADMINISTRACIÓN, PERO SÍ PUEDA CAMBIARSE EL NOMBRE, **SE DEBE CONSIDERAR QUE EL IDENTIFICADOR NUMÉRICO DEL USUARIO NO SE PUEDE CAMBIAR**, Y PODRÍA EMPLEARSE EN UN ATAQUE.

# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. **CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS**
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## 3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

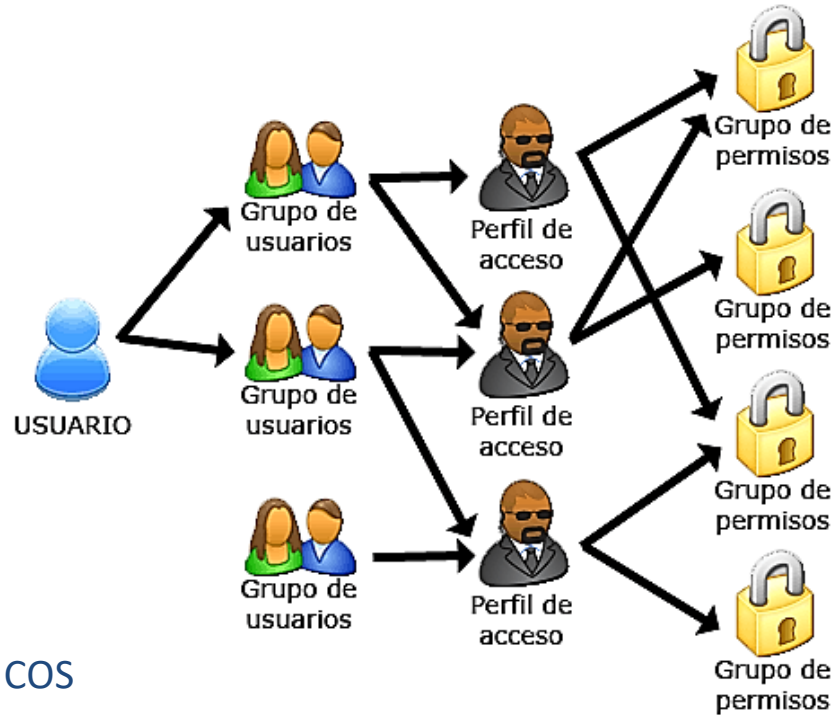
**LAS CONTRASEÑAS DEBEN CUMPLIR UNOS REQUISITOS MÍNIMOS**, O POR EL CONTRARIO RESULTAN INVÁLIDAS. ENTRE LOS **ASPECTOS A CONSIDERAR** ESTÁN:

- *LA LONGITUD*
- *LA VARIEDAD DE CARACTERES EMPLEADOS*
- *EL PERIODO E VIGENCIA*
- *NO PERMITIR LA COINCIDENCIA CON LAS CLAVES ANTERIORES.*

ESTAS CONDICIONES DE COMPLEJIDAD SE AGRUPAN, FORMANDO UNA **DIRECTIVA DE GESTIÓN DE CONTRASEÑAS**.

# 3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

TAMBIÉN **DEBEN GESTIONARSE LOS PRIVILEGIOS DE LOS USUARIOS**, LO QUE NORMALMENTE SE REALIZA MEDIANTE LA **INCLUSIÓN O EXCLUSIÓN DE LOS USUARIOS EN LOS GRUPOS CON PERMISOS CONFIGURADOS** SOBRE UNOS FICHEROS O PROGRAMAS.



# 3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

LA NORMA **ISO 17799:2005** ESTABLECE EN SU CONTROL **GESTIÓN DE PRIVILEGIOS**, QUE *SE DEBE RESTRINGIR Y CONTROLAR LA ASIGNACIÓN Y USO DE PRIVILEGIOS MEDIANTE UN PROCESO DE AUTORIZACIÓN FORMAL*, QUE CONTEMPLE:

- IDENTIFICAR A QUE USUARIOS HAY QUE DAR ACCESO A CADA RECURSO.
- LOS PRIVILEGIOS DEBEN OTORGARSE EN BASE A LA NECESIDAD DE SABER.
- MANTENER PROCESO DE AUTORIZACIÓN Y REGISTRO, Y NO OTORGARLOS HASTA QUE SE COMPLETE.
- ES PREFERIBLE EL EMPLEO DE RUTINAS, U OTROS MECANISMOS AUTOMÁTICOS DEL SISTEMA, QUE EVITEN LA NECESIDAD DE OTORGAR PRIVILEGIOS.
- ES PREFERIBLE USAR PROGRAMAS QUE EVITEN LA NECESIDAD DE EJECUTARSE CON PRIVILEGIOS.
- LOS PRIVILEGIOS DEBEN OTORGARSE A UN IDENTIFICADOR DE USUARIO, DIFERENTE DEL UTILIZADO EN EL USO NORMAL Y DIARIO DE LA EMPRESA.

## 3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

SOBRE LAS CONDICIONES QUE DEBEN CUMPLIR LAS CONTRASEÑAS, LA NORMA **ISO 17799:2005** ESTABLECE EN EL CONTROL **USO DE CLAVES SECRETAS**, QUE DEBEN SER DE CALIDAD, CON LONGITUD SUFICIENTE Y QUE ADEMÁS CUMPLAN:

- QUE SEAN FÁCILES DE RECORDAR.
- QUE NO SE BASEN EN NADA FÁCILMENTE ADIVINABLE COMO INFORMACIÓN DE LA PERSONA.
- QUE NO INCLUYAN PALABRAS INCLUIDAS EN DICCIONARIOS.
- QUE ESTÉN LIBRES DE CARACTERES CONSECUTIVOS IDÉNTICOS, TODOS NUMÉRICOS O ALFANUMÉRICOS.
- QUE SE CAMBIEN REGULARMENTE, O EN BASE AL NÚMERO DE ACCESOS, EVITANDO REUTILIZAR DE CLAVES ANTERIORES.

# 3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

## DIRECTRICES EN GUÍAS NIST

LA GUÍA **NIST 800-123** (SEGURIDAD GENERAL DE SERVIDORES) ESTABLECE QUE LAS REGLAS O POLÍTICA DE CONTRASEÑAS DEBE FIJAR:

1. LA LONGITUD MÍNIMA,
2. LA COMPLEJIDAD, EMPLEANDO MEZCLA DE DIFERENTES TIPOS DE CARACTERES PARA REDUCIR EL POSIBLE ÉXITO DE UN ATAQUE DE ENSAYO DE ERROR DE PALABRAS CONTENIDAS EN DICCIONARIOS,
3. EL PERIODO DE VALIDEZ DE UNA CONTRASEÑA,
4. LA REUTILIZACIÓN DE CONTRASEÑAS QUE EVITE EMPLEAR LAS ANTERIORES,
5. LA AUTORIDAD PARA CAMBIAR O RESTABLECER LAS CONTRASEÑAS, Y
6. LA SEGURIDAD DE LAS CONTRASEÑAS EN LO REFERENTE A QUE SE ALMACENEN CIFRADAS EN EL SERVIDOR, E INCLUSO QUE SE USEN CLAVES DIFERENTES PARA LA ADMINISTRACIÓN DEL SERVIDOR, Y PARA OTRAS LABORES DE ADMINISTRACIÓN.

# 3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

## DIRECTRICES EN GUÍAS NIST

LA GUÍA **NIST 800-123** TAMBIÉN INDICA QUE SE DEBEN **APLICAR MEDIDAS PARA PREVENIR QUE LA CONTRASEÑA SE ACABE ADIVINANDO POR MERA REPETICIÓN** (FUERZA BRUTA O ATAQUES BASADOS DE DICCIONARIOS).

PARA EVITARLO, EL SISTEMA DEBE **INCREMENTAR PAULATINAMENTE EL TIEMPO ENTRE INTENTOS DE INICIO DE SESIÓN**, DE FORMA QUÉ A CADA FALLO, EL SIGUIENTE INTENTO NECESITE ESPERAR MÁS TIEMPO.

# 3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

## DIRECTRICES EN GUÍAS NIST

SI ESTO NO ES POSIBLE, **DESPUÉS DE UN NÚMERO DE INTENTOS DE ACCESO FALLIDOS, LA CUENTA DEBE BLOQUEARSE BIEN POR UN PERIODO DE TIEMPO, BIEN DE MANERA PERMANENTE**, HASTA QUE UN USUARIO CON PRIVILEGIOS LA DESBLOQUEE.

EN ESTA CONFIGURACIÓN TAMBIÉN **EXISTE UN COMPROMISO ENTRE SEGURIDAD Y CONVENIENCIA,** PORQUE SUCESIVOS INTENTOS DE INICIO DE SESIÓN PUEDEN ACABAR BLOQUEANDO LAS CUENTAS, LO QUE INDIRECTAMENTE PRODUCE UNA DENEGACIÓN DE SERVICIO A LOS USUARIOS LÍCITOS.

# 3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

## DIRECTRICES EN GUÍAS NIST

DEBE PONERSE ESPECIAL ATENCIÓN EN QUE **LA CUENTA DEL USUARIO CON MÁXIMOS PRIVILEGIOS NO IMPIDA EL INICIO DE SESIÓN MEDIANTE LA CONSOLA LOCAL**, ASÍ COMO EN QUE SE REGISTREN TODOS LOS INTENTOS DE INICIO DE SESIÓN.

OTRAS MEDIDAS ADICIONALES, DEPENDIENDO DEL VALOR DE LA INFORMACIÓN ALMACENADA, PUEDEN SER EL **EMPLEO DE TARJETAS INTELIGENTES, LECTORES BIOMÉTRICOS, O SISTEMAS DE CONTRASEÑA DE UN SOLO USO**.

# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. **ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES**
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

SE ABORDA AHORA EL **ANÁLISIS DE LAS CONSIDERACIONES DE SEGURIDAD** QUE SE DEBEN OBSERVAR **EN LAS APLICACIONES QUE PERMANEZCAN INSTALADAS EN LOS SISTEMAS**, Y ESPECÍFICAMENTE, EN LAS IMPLICACIONES PARA CON LAS COMUNICACIONES QUE ELLO PUEDA ACARREAR.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## HERRAMIENTAS Y OTRAS APLICACIONES.

ES UNA CUESTIÓN PRIMORDIAL **ELIMINAR TODAS LAS HERRAMIENTAS, UTILIDADES, APLICACIONES, Y SERVICIOS QUE NO SEAN ESTRICTAMENTE NECESARIOS**.

PARA ELLO SE PRECISAN **MEDIDAS TÉCNICAS DE REVISIÓN, Y DESINSTALACIÓN** DE APLICACIONES INNECESARIAS; Y **MEDIDAS NORMATIVAS QUE REGULEN LA INSTALACIÓN** DE SOFTWARE.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## HERRAMIENTAS Y OTRAS APLICACIONES

LA NORMA **ISO 17799:2005** APORTA LAS SIGUIENTES PAUTAS:

- **SE DEBEN CONTROLAR LOS CAMBIOS CON PROCEDIMIENTOS FORMALES** PARA MINIMIZAR LA CORRUPCIÓN DE LOS SISTEMAS. LA INTRODUCCIÓN DE NUEVOS SISTEMAS, O LAS MODIFICACIONES DE LOS EXISTENTES, DEBEN HACERSE SEGÚN UN PROCESO DE: DOCUMENTACIÓN, ESPECIFICACIÓN, PRUEBA, CONTROL DE CALIDAD, Y PUESTA EN MARCHA. SOBRE TODO, EL SOFTWARE NUEVO DEBE PROBARSE EN UN ENTORNO SEPARADO.
- **DEBEN EVITARSE OPORTUNIDADES COMO LAS QUE OFRECEN EL USO Y EXPLOTACIÓN DE PUERTOS O CANALES** DE MANERA DISIMULADA, O ENCUBIERTA POR ALGUNAS APLICACIONES. SE RECOMIENDA **ANALIZAR EL TRÁFICO DEL EQUIPO, Y HACER USO DE APLICACIONES CONSIDERADOS DE LA MÁS ALTA INTEGRIDAD**, Y SIEMPRE EVALUADAS PREVIAMENTE.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## HERRAMIENTAS Y OTRAS APLICACIONES

- **SE DEBE DISUADIR A LOS USUARIOS DE EMPLEAR LOS MEDIOS DE PROCESAMIENTO DE LA INFORMACIÓN PARA PROPÓSITOS NO AUTORIZADOS**, LO QUE INCLUYE EL EMPLEO DE UTILIDADES NO PERMITIDAS PARA FINES NO AUTORIZADOS.
- **SE PROHÍBE LA REPRODUCCIÓN, MODIFICACIÓN, TRANSFORMACIÓN, CESIÓN, COMUNICACIÓN, O USO FUERA DE LA EMPRESA DE LOS PROGRAMAS Y APLICACIONES INFORMÁTICAS INSTALADAS EN LOS EQUIPOS QUE PERTENECEN A LA EMPRESA.**
- **NO SE PODRÁN DESHABILITAR O ELIMINAR LAS APLICACIONES INSTALADAS POR LA EMPRESA, ESPECIALMENTE LAS RELACIONADAS CON LA SEGURIDAD.**

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## HERRAMIENTAS Y OTRAS APLICACIONES

LA GUÍA **CCN-STIC 821** PROPONE LAS SIGUIENTES MEDIDAS ORGANIZATIVAS GENÉRICAS SOBRE LA INSTALACIÓN DE SOFTWARE:

- **SOLO EL PERSONAL DE SOPORTE TÉCNICO AUTORIZADO PODRÁ INSTALAR SOFTWARE EN LOS EQUIPOS INFORMÁTICOS O DE COMUNICACIONES DE LOS USUARIOS**, CON LA EXCEPCIÓN DE LAS HERRAMIENTAS DE USO COMÚN, QUE PUEDAN SER DESCARGABLES DESDE SERVIDORES INTERNOS.
- **LOS USUARIOS PODRÁN SOLICITAR LA INCLUSIÓN DE UNA APLICACIÓN**, LO QUE DEBE SER ESTUDIADO, AL MENOS POR EL PERSONAL TÉCNICO DE SEGURIDAD.
- **NO SE PODRÁ INSTALAR SOFTWARE QUE NO DISPONGA DE LICENCIA CORRESPONDIENTE**, **O** CUYA UTILIZACIÓN **NO SEA CONFORME CON LA LEGISLACIÓN VIGENTE** EN MATERIA DE **PROPIEDAD INTELECTUAL**.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## HERRAMIENTAS Y OTRAS APLICACIONES

- **SE PROHÍBE LA REPRODUCCIÓN, MODIFICACIÓN, TRANSFORMACIÓN, CESIÓN, COMUNICACIÓN, O USO FUERA DE LA EMPRESA DE LOS PROGRAMAS Y APLICACIONES INFORMÁTICAS INSTALADAS** EN LOS EQUIPOS QUE PERTENECEN A LA EMPRESA.
- **NO SE PODRÁN DESHABILITAR O ELIMINAR LAS APLICACIONES INSTALADAS POR LA EMPRESA**, ESPECIALMENTE LAS RELACIONADAS CON LA SEGURIDAD.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## COMUNICACIONES Y PUERTOS DE RED

**SE DEBEN IDENTIFICAR LOS SERVICIOS QUE SON ACCESIBLES DESDE FUERA DE LA EMPRESA**, PARA HABILITAR EL TRÁFICO ENTRANTE EXCLUSIVAMENTE EN LOS PUERTOS QUE NECESITEN ESOS SERVICIOS.

LA NORMA **ISO 17799:2005** DISPONE VARIAS CONTRAMEDIDAS DE CARÁCTER ESPECIAL:

- **LOS USUARIOS SÓLO DEBERÍAN TENER ACCESO A LOS SERVICIOS PARA LOS CUALES HAYAN SIDO AUTORIZADOS**.
- EN LOS PUERTOS HABILITADOS **EL ACCESO DEBE MANTENERSE AUTENTICADO** (EMPLEANDO TÉCNICAS DE CRIPTOGRAFÍA, DISPOSITIVOS HARDWARE O UN MECANISMO DE DESAFÍO/RESPUESTA, O REDES PRIVADAS VIRTUALES).

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## COMUNICACIONES Y PUERTOS DE RED

- LOS SISTEMAS Y/O GRUPOS DE USUARIOS DEBEN **SEPARARSE EN DIFERENTES REDES.**
- SE DEBE **RESTRINGIR LA CAPACIDAD DE CONEXIÓN DE LOS USUARIOS A LA RED**, EMPLEANDO, POR EJEMPLO, PASARELAS DE RED O GATEWAYS, CON TABLAS O REGLAS PREDEFINIDAS PARA RESTRINGIR EL USO DEL CORREO, LA TRANSFERENCIA DE ARCHIVOS, EL ACCESO PARA INICIAR UNA SESIÓN INTERACTIVA REMOTA, O EL ACCESO A UNA APLICACIÓN CONCRETA.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## COMUNICACIONES Y PUERTOS DE RED

LA GUÍA **CCN-STIC 821** ESTABLECE UNA **NORMATIVA** QUE LAS EMPRESAS PODRÍAN APLICAR **PARA CONTROLAR EL USO DE INTERNET**. LAS **MEDIDAS QUE DEBEN CONOCER Y ACEPTAR POR ESCRITO TODOS LOS USUARIOS**, SON:

- USAR INTERNET PARA FINES PROFESIONALES.
- NO VISITAR PÁGINAS DE CONTENIDO POCO ÉTICO, OFENSIVO O ILEGAL.
- NO VISITAR PÁGINAS NO FIABLES O SOSPECHOSAS.
- CUIDAR LA INFORMACIÓN QUE SE PUBLICA EN INTERNET.
- OBSERVAR LAS RESTRICCIONES LEGALES QUE SEAN DE APLICACIÓN.
- REALIZAR DESCARGAS SOLO SI SE TIENE AUTORIZACIÓN.
- NO DESCARGAR CÓDIGO O PROGRAMAS NO CONFIABLES.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## COMUNICACIONES Y PUERTOS DE RED

- ASEGURAR LA AUTENTICIDAD DE LA PÁGINA VISITADA.
- COMPROBAR LA SEGURIDAD DE LA CONEXIÓN.
- CERRAR LAS SESIONES AL TERMINAR LA CONEXIÓN.
- UTILIZAR HERRAMIENTAS CONTRA CÓDIGO DAÑINO.
- MANTENER ACTUALIZADO EL NAVEGADOR Y LAS HERRAMIENTAS DE SEGURIDAD.
- UTILIZAR LOS NIVELES DE SEGURIDAD DEL NAVEGADOR.
- ELIMINAR LA INFORMACIÓN PRIVADA.
- NO INSTALAR COMPLEMENTOS DESCONOCIDOS.
- LIMITAR Y VIGILAR LA EJECUCIÓN DE PROGRAMAS EN EL NAVEGADOR COMO APPLETS Y SCRIPTS.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## COMUNICACIONES Y PUERTOS DE RED

ADEMÁS, LA GUÍA ESTABLECE QUE **LOS PUERTOS AUTORIZADOS**, A PRIORI**, DEBEN SER UN CONJUNTO MÍNIMO ESTÁNDAR**, COMO:

- HTTP, SERVICIO WEB ESTÁNDAR, POR EJEMPLO, EN EL PUERTO 80.
- HTTPS, SERVICIO WEB SEGURO, POR EJEMPLO, EN EL PUERTO 443.
- FTP, SERVICIO DE TRANSFERENCIA DE FICHEROS, POR EJEMPLO, EN TCP/21.
- SERVICIOS VARIOS DE LA EMPRESA, IDENTIFICADOS Y DEFINIDOS.

ESTABLECE TAMBIÉN QUE, **DE REQUERIRSE OTROS PUERTOS, SU INCLUSIÓN DEBE SOLICITARSE Y ANALIZARSE,** AL MENOS POR EL PERSONAL TÉCNICO DE SEGURIDAD.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## PASARELAS DE SEGURIDAD

UNA **PASARELA, PUERTA DE ENLACE O PUERTA DE ACCESO (GATEWAY)** ES UN EQUIPO DE COMUNICACIONES QUE **INTERCONECTA REDES CON ARQUITECTURAS DIFERENTES**, REALIZANDO PARA ELLO FUNCIONES AVANZADAS DE TRADUCCIÓN DE PROTOCOLOS ENTRE AMBAS REDES.

EN EL ÁMBITO DE INTERNET Y DE REDES TCP/IP, **FRECUENTEMENTE UNA PASARELA SOLO REALIZA FUNCIONES DE ENCAMINAMIENTO** (**ROUTER**) E INTERCONEXIÓN DE REDES, LO QUE SIMPLIFICA EL EQUIPO A FUNCIONES DE LA CAPA DE INTERNET.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## PASARELAS DE SEGURIDAD

NORMALMENTE, LA EMPRESA EMPLEARÁ ARQUITECTURA DE RED TCP/IP, Y ESTARÁ CONECTADA A INTERNET, DE MANERA QUE LAS PASARELAS SERÁN DISPOSITIVOS QUE EXTIENDAN LAS FUNCIONES DE UN ROUTER.

TAL ES EL CASO DE LAS **PASARELAS DE SEGURIDAD**, QUE AÑADEN NORMALMENTE **SERVICIOS DE ANTIVIRUS O DE DETECCIÓN DE INTRUSOS**, PARA TOMAR DECISIONES SOBRE LAS CONEXIONES QUE SE PERMITEN.

USO DE **FIREWALLS,** COMO OTRAS MEDIDAS DE SEGURIDAD YA VISTAS, PLANTEA UN **BALANCE ENTRE LA FUNCIONALIDAD** DE PERMITIRLO TODO**, Y LA SEGURIDAD** DE RESTRINGIRLO TODO.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## DIRECTRICES EN GUÍAS NIST

LA GUÍA **NIST 800-123** EN SU APARTADO 4.2.1, INDICA QUE, IDEALMENTE, **UNA APLICACIÓN DE SERVIDOR DEBERÍA ESTAR EN UN EQUIPO U ORDENADOR DEDICADO A ESTA ÚNICA FUNCIÓN.**

CUANDO SE INSTALE **EL SISTEMA OPERATIVO, DEBE REALIZARSE UNA INSTALACIÓN MÍNIMA**, PARA POSTERIORMENTE AÑADIR TODOS LOS SERVICIOS Y APLICACIONES QUE SE NECESITEN.

EL **ENFOQUE CONTRARIO** (SI NO ES POSIBLE REALIZAR UNA INSTALACIÓN MÍNIMA) CONSISTE **EN ELIMINAR TODAS LAS APLICACIONES, SERVICIOS Y PROTOCOLOS DE RED INNECESARIOS** TRAS LA INSTALACIÓN ESTÁNDAR.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## DIRECTRICES EN GUÍAS NIST

**DESINSTALAR ES SIEMPRE PREFERIBLE A DESACTIVAR O BLOQUEAR**, PORQUE AQUELLO QUE NO EXISTE NO TIENE VULNERABILIDAD ALGUNA.

NO OBSTANTE, **SI ALGO NO SE PUEDE DESINSTALAR, PUEDE BLOQUEARSE**, Y EN LA MEDIDA DE LO POSIBLE, HACERLO DE FORMA QUE VOLVER A HABILITARLO PRECISE DE INTERVENCIÓN FÍSICA INTENCIONADA.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## DIRECTRICES EN GUÍAS NIST

LOS **SERVICIOS QUE SE DEBEN REVISAR EXPRESAMENTE** SON:

- SERVICIOS PARA COMPARTIR ARCHIVOS E IMPRESORAS.
- SERVICIOS DE COMUNICACIONES INALÁMBRICAS.
- SERVICIOS DE CONTROL Y ACCESO REMOTO, ESPECIALMENTE LOS NO CIFRADOS, COMO ES EL CASO DE TELNET.
- SERVICIOS DE DIRECTORIO (LDAP).
- SERVIDORES WEB.
- SERVIDORES DE CORREO ELECTRÓNICO.
- COMPILADORES Y LIBRERÍAS DE LENGUAJES.
- HERRAMIENTAS DE DESARROLLO.
- HERRAMIENTAS Y UTILIDADES DE GESTIÓN DE RED.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## DIRECTRICES EN GUÍAS NIST

SE RECOMIENDA **ELIMINAR TODA LA DOCUMENTACIÓN DEL FABRICANTE DEL SERVIDOR**, ASÍ COMO TODOS LOS **ARCHIVOS DE EJEMPLO** O **TEST** QUE PUEDAN INCORPORAR LAS APLICACIONES Y LOS COMPILADORES QUE PUEDEN ESTAR PRESENTES.

**LOS SERVICIOS** QUE DEBAN PERMANECER EN EL SERVIDOR **DEBEN CONFIGURARSE PARA QUE SOLO ACEPTEN CONEXIONES EN LOS PUERTOS TCP/UDP PREVISTOS**, NO EN OTROS.

# 4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

## DIRECTRICES EN GUÍAS NIST

ENTRE LAS **VENTAJAS** DE **DESHABILITAR SERVICIOS INNECESARIOS**, ESTÁ EL **AUMENTAR LA SEGURIDAD DEL RESTO DE SERVICIOS** HABILITADOS, PORQUE SE **REDUCE LA SUPERFICIE DE ATAQUE**, Y PORQUE **SE REDUCEN POSIBLES PROBLEMAS DE DISPONIBILIDAD** DERIVADOS DE INCOMPATIBILIDADES O FALLOS EN LOS SERVICIOS DESINSTALADOS,

ADEMÁS DE LA **LIBERACIÓN DE RECURSOS DEL SISTEMA** PARA LOS SERVICIOS QUE VERDADERAMENTE SE NECESITAN, Y POR SUPUESTO, LA MENOR NECESIDAD DE ESPACIO EN DISCO PARA CONSERVAR LOS LOGS DE LOS SERVICIOS EN EJECUCIÓN.

# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. **CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE**
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

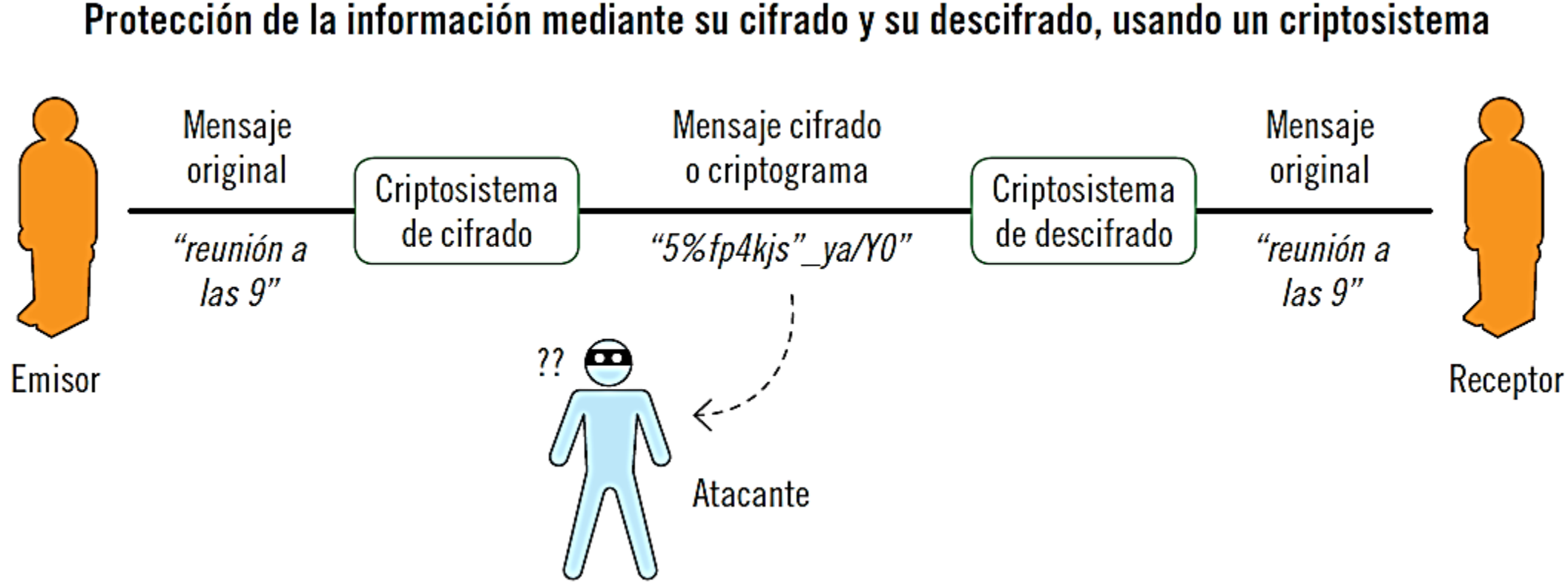
## 5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE

**ALGUNOS DE LOS SERVICIOS** QUE SE PRESTAN A TRAVÉS DE INTERNET **NO SON SEGUROS**, SI LA INFORMACIÓN QUE SE ENVÍA NO VIAJA CIFRADA.

SE RECURRE AL EMPLEO DE **MECANISMOS QUE CIFREN LA INFORMACIÓN** INTERCAMBIADA, DE MANERA QUE, SI UN ATACANTE OBTUVIERA ACCESO AL TRÁFICO, TENDRÍA QUE DESCIFRAR LA INFORMACIÓN PARA ACCEDER A ELLA.

DE ESTA MANERA, **LA INFORMACIÓN VIAJA PROTEGIDA**, Y OFRECE RESISTENCIA A CONOCER SU VALOR. EN EL EXTREMO OPUESTO DE LA COMUNICACIÓN, **EL DESTINATARIO DESCIFRA LA INFORMACIÓN**, Y ACCEDE AL CONTENIDO.

# 5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE



# 5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE

## PROTOCOLOS SEGUROS

**EL EMPLEO DE CRIPTOSISTEMAS OTORGA SEGURIDAD A LAS COMUNICACIONES Y SERVICIOS**, EN MAYOR O MENOR MEDIDA, SEGÚN LA COMPLEJIDAD DE LAS MEDIDAS TÉCNICAS APLICADAS (CIFRADO SIMÉTRICO O ASIMÉTRICO, EMPLEO DE FIRMAS ELECTRÓNICAS, DE FIRMAS DIGITALES, E INCLUSO DE CERTIFICADOS DIGITALES).

**LOS DIFERENTES PROTOCOLOS DE LOS SERVICIOS DE INTERNET HACEN USO DE ESTAS TÉCNICAS, DE MANERA QUE SE OBTIENEN SUS VARIANTES SEGURAS**. A CONTINUACIÓN, SE RESUMEN LOS MÁS HABITUALES PARA EL SERVICIO WEB, LA CONEXIÓN REMOTA Y TRANSFERENCIA DE FICHEROS, Y PARA EL CORREO ELECTRÓNICO.

# 5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE

## PROTOCOLOS SEGUROS

### HTTPS EN LUGAR DE HTTP

**HTTPS (HYPERTEXT TRANSFER PROTOCOL SECURE)** ES EL RESULTADO DE AÑADIR AL PROTOCOLO **HTTP** ESTÁNDAR PARA NAVEGACIÓN WEB LAS PRESTACIONES DE CIFRADO **SSL (SECURE SOCKET LAYER), Y DE SU SUCESOR TLS (TRANSPORT LAYER SECURITY),** QUE SON PROTOCOLOS DE LA CAPA DE TRANSPORTE.

ESTA COMBINACIÓN **PERMITE ASEGURAR QUE EL SERVICIO LO OFRECE UN SERVIDOR WEB AUTÉNTICO** (*NO UN IMPOSTOR*) **Y** QUE **LAS COMUNICACIONES CON ESTE SERVIDOR ESTÁN PROTEGIDAS**.

# 5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE

## PROTOCOLOS SEGUROS

### SSH EN LUGAR DE TELNET, Y SFTP EN LUGAR DE FTP

**SSH (SECURE SHELL)** ES UN PROTOCOLO SEGURO, QUE PERMITE **INICIAR SESIÓN EN SISTEMAS REMOTOS**, EMPLEANDO MECANISMO DE CLAVE ASIMÉTRICA.

TAMBIÉN SE EMPLEA **SSH PARA TRANSFERENCIA DE FICHEROS**, EN LO QUE SE DENOMINA **SFTP**, Y QUE SE RECOMIENDA EMPLEAR PARA REEMPLAZAR EL USO DE FTP.

EXISTEN APLICACIONES DE LIBRE DISTRIBUCIÓN, COMO LA APLICACIÓN **PUTTY**, QUE PERMITEN ESTOS SERVICIOS.

# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. **ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS**
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

# 6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

## ACTUALIZACIÓN DE PARCHES

AUNQUE SE MINIMICE EL NÚMERO DE SERVICIOS IMPLEMENTADOS, Y SE EMPLEEN PROTOCOLOS SEGUROS, **LAS FUNCIONES PRESENTAN VULNERABILIDADES**.

ESTAS VULNERABILIDADES, **CUANDO SON DESCUBIERTAS, SUPONEN UN RIESGO PARA EL SISTEMA DE INFORMACIÓN** QUE LO IMPLEMENTA. HABITUALMENTE, EL FABRICANTE DE LA APLICACIÓN O SERVICIO SUELE TENER CONOCIMIENTO DE LA VULNERABILIDAD EN UNA FASE MUY TEMPRANA DESDE SU DESCUBRIMIENTO.

# 6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

## ACTUALIZACIÓN DE PARCHES

ES A PARTIR DE ESE MOMENTO CUANDO **EL FABRICANTE TRABAJA ACTIVAMENTE PARA CORREGIR LA DEBILIDAD** DE SU PRODUCTO, **Y PONER A DISPOSICIÓN** DE SUS USUARIOS **EL PARCHE O CORRECCIÓN** QUE DEBEN APLICAR PARA SUBSANAR EL PROBLEMA.

**EL USUARIO DEBE APLICAR EL PARCHE PARA ROBUSTECER SU SISTEMA** DE INFORMACIÓN.

# 6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

## ACTUALIZACIÓN DE PARCHES

LA NORMA **ISO 17799:2005** ESTABLECE UNA CONTRAMEDIDA RELATIVA AL *CONTROL DE LAS VULNERABILIDADES TÉCNICAS*.

**SE DEBE OBTENER INFORMACIÓN OPORTUNA SOBRE LAS DEBILIDADES DE LOS SISTEMAS DE INFORMACIÓN QUE SE ESTÉN USANDO**.

PARA ELLO, SE DEBE PARTIR DE UN **INVENTARIO ACTUALIZADO Y COMPLETO DE LAS APLICACIONES** QUE DETALLE EL FABRICANTE, LAS VERSIONES, Y LAS PERSONAS RESPONSABLES DE LA APLICACIÓN.

# 6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

## ACTUALIZACIÓN DE PARCHES

RECOMIENDA QUE SE ESTABLEZCA UN **PROCEDIMIENTO FORMAL DE GESTIÓN DE LAS VULNERABILIDADES**, QUE INCLUYA:

- BÚSQUEDA ACTIVA DE INFORMACIÓN, Y MONITORIZACIÓN DE APARICIÓN DE NUEVAS VULNERABILIDADES
- ESTABLECIMIENTO DE UN CRONOGRAMA, PARA REACCIONAR A LAS NUEVAS VULNERABILIDADES APARECIDAS.
- LA EVALUACIÓN DEL RIESGO VINCULADO A LA VULNERABILIDAD APARECIDA PARA DETERMINAR LAS ACCIONES A EMPRENDER, COMO APLICAR UN PARCHE, O CORRECCIÓN A LA APLICACIÓN.
- SE DEBE CONSIDERAR EL RIESGO DE APLICAR UN PARCHE FRENTE AL DE NO APLICARLO. ANTES DE APLICARLO, PREFERIBLEMENTE SE DEBERÍA PROBAR Y EVALUAR SU EFECTIVIDAD, Y AUSENCIA DE EFECTOS SECUNDARIOS.

# 6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

## ACTUALIZACIÓN DE PARCHES

**OTROS CONTROLES** ALTERNATIVOS A LA APLICACIÓN DE UN PARCHE PUEDEN SER:

- DESCONECTAR SERVICIOS RELACIONADOS CON LA VULNERABILIDAD.
- AGREGAR CONTROLES COMO FIREWALLS EN EL PERÍMETRO DE SEGURIDAD.
- REFORZAR LA MONITORIZACIÓN PARA DETECTAR O EVITAR ATAQUES
- MANTENER REGISTROS DE AUDITORÍA DE LOS PROCEDIMIENTOS REALIZADOS.
- REVISIÓN Y EVALUACIÓN DEL PROCESO DE GESTIÓN DE VULNERABILIDADES.
- ATENDER PRIMERO LOS SISTEMAS DE MAYOR RIESGO.

# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. **PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO**
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

EL **CÓDIGO MALICIOSO** ES UNA **AMENAZA CONSTANTE** PARA LOS SISTEMAS DE INFORMACIÓN.

SE TRATA DE APLICACIONES QUE, UNA VEZ EJECUTADAS, PRODUCEN UN DAÑO INTENCIONADO AL SISTEMA DE INFORMACIÓN.

POR EJEMPLO, PROPORCIONAN UNA VÍA DE ACCESO A UN ATACANTE, BORRAN UN ARCHIVO, O LO ENVÍAN A UN SERVIDOR REMOTO.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## ATAQUE DE CÓDIGO MALICIOSO

PARA QUE LA AMENAZA DEL CÓDIGO MALICIOSO SE MATERIALICE, DEBE OCURRIR QUE LLEGUE A UN EQUIPO DE LA RED, Y QUE SEA EJECUTADA POR EL MISMO.


**LA VÍA DE ACCESO** AL SISTEMA DE INFORMACIÓN PUEDE SER BIEN **INTERNET**, BIEN UN **MEDIO DE ALMACENAMIENTO** COMO UN CD-ROM, O UNIDAD USB.

**DEBEN APLICARSE SISTEMAS QUE DETECTEN LOS CÓDIGOS MALICIOSOS** EN TODOS LOS PUNTOS DE CONEXIÓN A INTERNET, Y EN TODOS LOS EQUIPOS QUE ADMITAN MEDIOS DE ALMACENAMIENTO EXTERNO.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## ATAQUE DE CÓDIGO MALICIOSO

**ESTA DETECCIÓN ES COMPLEJA**, PORQUE EL CÓDIGO MALICIOSO PUEDE FORMAR PARTE DE OTRA APLICACIÓN LÍCITA, O BIEN TRANSPORTARSE DE MANERA CIFRADA, A LO QUE SE SUMA LA DIFICULTAD DE LA ENORME VARIEDAD DE SOFTWARE MALICIOSO EXISTENTE.

PARA QUE LA APLICACIÓN SEA EJECUTADA, LAS INSTRUCCIONES DEL PROGRAMA DEBEN ESTAR EN LA MEMORIA VOLÁTIL DEL ORDENADOR, Y EL MICROPROCESADOR DEBE EJECUTARLAS.

**LA LABOR TAMBIÉN ES COMPLEJA**, SE DEBE ANALIZAR EL ESPACIO DE MEMORIA EN BUSCA DE UNA SECUENCIA DE INSTRUCCIONES CONOCIDAS DE LOS CÓDIGOS MALICIOSOS EXISTENTES.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## ATAQUE DE CÓDIGO MALICIOSO

LA NORMA ISO **27001** ESTABLECE UN OBJETIVO DE CONTROL DEDICADO A LA **PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE)**. **LA PROTECCIÓN SE BASARÁ EN**:

- UNA POLÍTICA FORMAL, QUE PROHÍBA EL USO DE SOFTWARE NO AUTORIZADO.
- LA IMPLANTACIÓN DE CONTROLES QUE PREVENGAN O DETECTEN EL USO DE SOFTWARE NO AUTORIZADO.
- LA IMPLANTACIÓN DE CONTROLES PARA PREVENIR O DETECTAR EL USO DE SITIOS WEB DE LOS QUE SE CONOCE O SOSPECHA SU CARÁCTER MALICIOSO.
- EL ESTABLECIMIENTO DE UNA POLÍTICA FORMAL PARA PROTEGER CONTRA LOS RIESGOS ASOCIADOS A LA OBTENCIÓN DE FICHEROS Y SOFTWARE.
- LA REDUCCIÓN DE VULNERABILIDADES QUE PODRÍAN SER EXPLOTADAS POR EL CÓDIGO MALICIOSO.

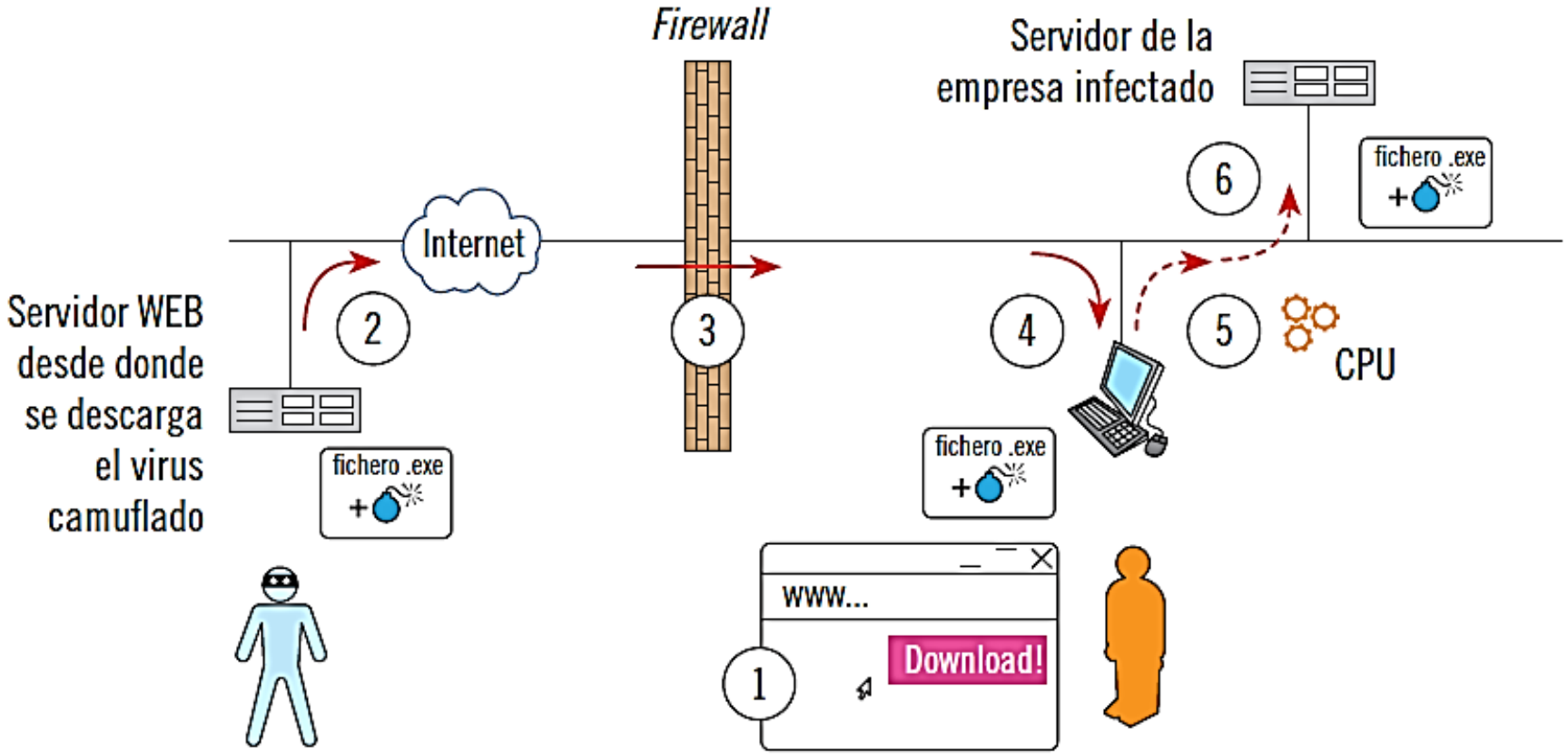
# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## ATAQUE DE CÓDIGO MALICIOSO

- LLEVAR A CABO REVISIONES REGULARES DEL SOFTWARE Y DATOS CONTENIDOS EN LOS SISTEMAS QUE SOPORTAN LOS PROCESOS CRÍTICOS DEL NEGOCIO.
- LA INSTALACIÓN Y ACTUALIZACIÓN DE SOFTWARE DE DETECCIÓN Y REPARACIÓN DE CÓDIGO MALICIOSO PARA ESCANEAR LOS ORDENADORES Y LOS DISPOSITIVOS.
- DEFINIR PROCEDIMIENTOS Y RESPONSABILIDADES DE GESTIÓN PARA TRATAR LA PROTECCIÓN DE LOS SISTEMAS CONTRA EL CÓDIGO MALICIOSO.
- PREPARAR PLANES ADECUADOS DE CONTINUIDAD DE NEGOCIO PARA LA RECUPERACIÓN DE LOS ATAQUES DE CÓDIGO MALICIOSO.
- IMPLANTAR PROCEDIMIENTOS PARA RECOGIDA DE INFORMACIÓN SOBRE NUEVOS CÓDIGOS MALICIOSOS.
- IMPLANTAR PROCEDIMIENTOS PARA VERIFICAR LA INFORMACIÓN RELATIVA AL CÓDIGO MALICIOSO, Y ASEGURAR QUE LOS BOLETINES DE ALERTA SON PRECISOS E INFORMATIVOS.
- AISLAR LOS ENTORNOS CUANDO PUEDAN PRODUCIRSE IMPACTOS CATASTRÓFICOS.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## ATAQUE DE CÓDIGO MALICIOSO



# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

ES CÓDIGO MALICIOSO **TODA APLICACIÓN QUE SIN CONOCIMIENTO NI AUTORIZACIÓN DEL USUARIO GENERA UN DAÑO INTENCIONADO AL SISTEMA**.

SU **CLASIFICACIÓN** SUELE REALIZARSE POR SU **FORMA DE PROPAGACIÓN**, Y POR EL **DAÑO QUE PRODUCEN**.

CASI TODO EL CÓDIGO MALICIOSO COMPARTE UNA **CARACTERÍSTICA COMÚN**: ***SE TRATA DE APLICACIONES CAPACES DE COPIARSE A SÍ MISMAS*** *DE MANERA SIMILAR A UN VIRUS.*

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR SU FORMA DE PROPAGACIÓN

#### VIRUS

**INFECTAN A OTROS FICHEROS EJECUTABLES** O CON ALGUNA CAPACIDAD DE EJECUCIÓN. **HACE QUE SE ACTIVEN CUANDO SE EJECUTA EL ARCHIVO DONDE ESTÁN INCLUIDOS**, Y A PARTIR DE ESE MOMENTO **PUEDEN PERMANECER RESIDENTES EN MEMORIA O TERMINAR SU EJECUCIÓN** CUANDO ACABE LA DEL PROGRAMA DONDE ESTÁN INCLUIDOS.

DURANTE EL PERIODO DE ACTIVIDAD, **EL VIRUS INTENTARÁ SU PROPAGACIÓN A OTROS FICHEROS EJECUTABLES, Y CAUSAR EL DAÑO INTENCIONADO** PARA EL QUE FUE DISEÑADO Y CONSTRUIDO.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR SU FORMA DE PROPAGACIÓN

#### GUSANOS

**NO INFECTAN A OTROS FICHEROS EJECUTABLES**, SINO QUE CONSTITUYEN UN FICHERO POR SÍ MISMO. PERSIGUEN COMO **OBJETIVO SU MÁXIMA PROPAGACIÓN**, EMPLEANDO PARA ELLO VÍAS COMO EL CORREO ELECTRÓNICO, REDES DE INTERCAMBIO DE FICHEROS, APLICACIONES DE MENSAJERÍA, Y APLICACIONES DE CONVERSACIÓN O CHAT.

**NO MODIFICAN UN ARCHIVO EJECUTABLE**, Y **PARA ASEGURAR QUE SE ACTIVAN, MODIFICAN PARÁMETROS DEL SISTEMA** PARA QUE SE EJECUTEN AL INICIO.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR SU FORMA DE PROPAGACIÓN

#### TROYANOS

CARECEN DE MECANISMO PROPIO DE REPLICACIÓN, Y **SUELEN PROPAGARSE AL VISITAR UNA PÁGINA WEB**, ESTANDO **INCLUIDOS EN OTRAS APLICACIONES** APARENTEMENTE INOFENSIVAS, **O AL SER DESCARGADOS POR UN PROGRAMA MALICIOSO** QUE YA EXISTA EN EL SISTEMA.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

#### ADWARE

**APLICACIONES QUE MUESTRAN PUBLICIDAD NO DESEADA** AL USUARIO, APOYÁNDOSE GENERALMENTE EN FUNCIONALIDADES DE ESPÍA, QUE ENVÍAN INFORMACIÓN DE LOS HÁBITOS DE USO DEL ORDENADOR A UN SERVIDOR REMOTO PARA MOSTRAR UNA PUBLICIDAD U OTRA.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

#### BLOQUEADORES

**IMPIDEN LA EJECUCIÓN DE DETERMINADOS PROGRAMAS**, COMO ANTIVIRUS U OTROS PROGRAMAS DE SEGURIDAD, **O IMPIDEN EL ACCESO A DETERMINADAS PÁGINAS WEB**, GENERALMENTE LAS DIRECCIONES DE LAS PÁGINAS DONDE LOS ANTIVIRUS SE ACTUALIZAN O LAS PÁGINAS DONDE SE PODRÍA DAR LA ALARMA Y SOLUCIÓN PARA EL BLOQUEADOR.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

**BOMBAS LÓGICAS**

QUE **ACTÚAN BAJO UNA CIRCUNSTANCIA PROGRAMADA**, POR EJEMPLO, UNA FECHA, O BAJO CONTROL REMOTO.

**BROMA (JOKE)**

AL EJECUTARSE HACE PENSAR AL USUARIO QUE EL ORDENADOR SE VA A BORRAR, QUE ESTÁ AVERIADO, ETC.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

**BULO (HOAX)**

EN FORMA DE CORREO ELECTRÓNICO ENGAÑA AL DESTINATARIO EN RELACIÓN A LA EXISTENCIA DE UN NUEVO VIRUS, O ALGUNA OTRA INFORMACIÓN, SOLICITÁNDOLE QUE LO REENVÍE A TODOS SUS CONTACTOS.

**CAPTURADOR DE TECLADO (KEYLOGGER)**

REGISTRA TODAS LAS PULSACIONES LOGRANDO ASÍ OBTENER LAS CLAVES DE ACCESO A LOS SERVICIOS.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

**REDIRECCIONADOR (CLICKER)**

**REDIRECCIONA EL NAVEGADOR WEB DEL USUARIO A UNA PÁGINA EN CONCRETO**, POR EJEMPLO, A UNA PÁGINA FALSA DE UN BANCO, U OTROS SERVICIOS, COMO EL CORREO ELECTRÓNICO.

**CRIPTOVIRUS (RANSOMWARE)**

QUE **CIFRAN UN FICHERO O EQUIPO Y COACCIONAN AL USUARIO** A QUE PAGUE UN RESCATE PARA DESCIFRARLOS.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

**DESCARGADOR (EDOWNLOADER)**

QUE **ACCEDEN A INTERNET PARA DESCARGAR OTROS PROGRAMAS** NORMALMENTE MALICIOSOS.

**ESPÍA (SPYWARE),**

**ENVÍAN INFORMACIÓN DEL EQUIPO A UN EQUIPO REMOTO**, BIEN SEAN LAS PÁGINAS VISITADAS Y OTRA INFORMACIÓN SOBRE HÁBITOS DE USO, O DOCUMENTOS COMPLETOS.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

**EXPLOIT**

**EXPLOTAN UNA VULNERABILIDAD**, GENERALMENTE PARA TENER CONTROL REMOTO DEL SISTEMA INFECTADO, O TENER ACCESO NO AUTORIZADO AL SISTEMA.

**FRAUDE**

**SIMULAN UN COMPORTAMIENTO ANORMAL**, E INCITAN A LA COMPRA. GENERALMENTE, UN FALSO ANTIVIRUS U OTRA APLICACIÓN, QUE INFORMA QUE SE TIENE UN VIRUS, Y PUEDE ELIMINARSE COMPRANDO LA APLICACIÓN.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

**INSTALADOR (DROPPER)**

PERMITE LA INSTALACIÓN DE OTROS CÓDIGOS MALICIOSOS EN EL SISTEMA.

**LADRÓN DE CONTRASEÑAS (PASSWORD STEALER)**

ACCEDE A FICHEROS CONOCIDOS DEL SISTEMA, DONDE SE REGISTRAN USUARIOS Y SUS CONTRASEÑAS PARA ENVIARLOS AL ATACANTE.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

**PUERTA TRASERA (EN INGLÉS BACKDOOR)**

**PERMITE EL ACCESO AL SISTEMA OPERATIVO, APLICACIÓN O PÁGINA WEB, ELUDIENDO LOS CONTROLES DE ACCESO** QUE HAYA. LA FINALIDAD ES OBTENER INFORMACIÓN, ACCEDER A LOS FICHEROS, REINICIAR EL ORDENADOR, ETC.

**HERRAMIENTAS DE CONTROL TOTAL (ROOTKIT)**

**PERMITEN AL ATACANTE TOMAR EL CONTROL DEL SISTEMA COMO SU ADMINISTRADOR**, PERMITIENDO AL ATACANTE REMOTO HACER LO QUE DESEE.

# 7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

## TIPOS DE CÓDIGO MALICIOSO

### CLASIFICACIÓN POR DAÑO QUE PRODUCEN

#### SECUESTRADOR DEL NAVEGADOR (HIJACKER)

MODIFICA LA PÁGINA DE INICIO DEL NAVEGADOR, AÑADE BARRAS DE BOTONES, MODIFICA LAS DIRECCIONES DE PÁGINAS MÁS VISITADAS O FAVORITOS, GENERALMENTE CON LA FINALIDAD DE AUMENTAR LAS VISITAS A UNA PÁGINA DETERMINADA.

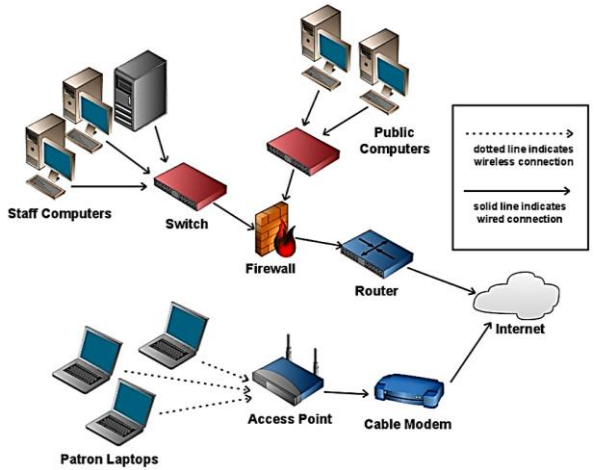
# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. **GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA**
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

**LA RED DE COMUNICACIONES** DE LA EMPRESA **ES LA INFRAESTRUCTURA QUE INTERCONECTA** AQUELLOS **ELEMENTOS QUE PRECISAN INTERCAMBIAR INFORMACIÓN** (ESTACIONES DE TRABAJO, CLIENTES, SERVIDORES, IMPRESORAS, ETC.)

LA GENERALIZACIÓN DE LAS REDES TCP/IP HACE QUE **SE PUEDAN CONECTAR OTROS MUCHOS DISPOSITIVOS A LA RED** (CÁMARAS WEB, DISPOSITIVOS MULTIMEDIA, UNIDADES DE DISCO DE RED, Y TODO TIPO DE SISTEMAS DEL ÁMBITO INDUSTRIAL).



# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

COMO MEDIDA PRINCIPAL PARA AUMENTAR LA SEGURIDAD, LOS SERVICIOS, SISTEMAS, Y USUARIOS, SE DEBEN **SEGREGAR EN REDES DIFERENTES** (*FÍSICAMENTE O LÓGICAMENTE*).

**LA ESTRUCTURA DE RED** QUE HABITUALMENTE SE TIENE ES DE **ÁRBOL-RAMA,** CREÁNDOSE GRUPOS POR CRITERIOS DE LOCALIZACIÓN.

ASÍ, LAS ESTACIONES DE TRABAJO DE LOS USUARIOS DE CADA PLANTA CONFLUYEN EN UN **SWITCH DE PLANTA** Y ESTOS CONFLUYEN A SU VEZ EN UN **SWITCH PRINCIPAL** PARA TODO EL EDIFICIO.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

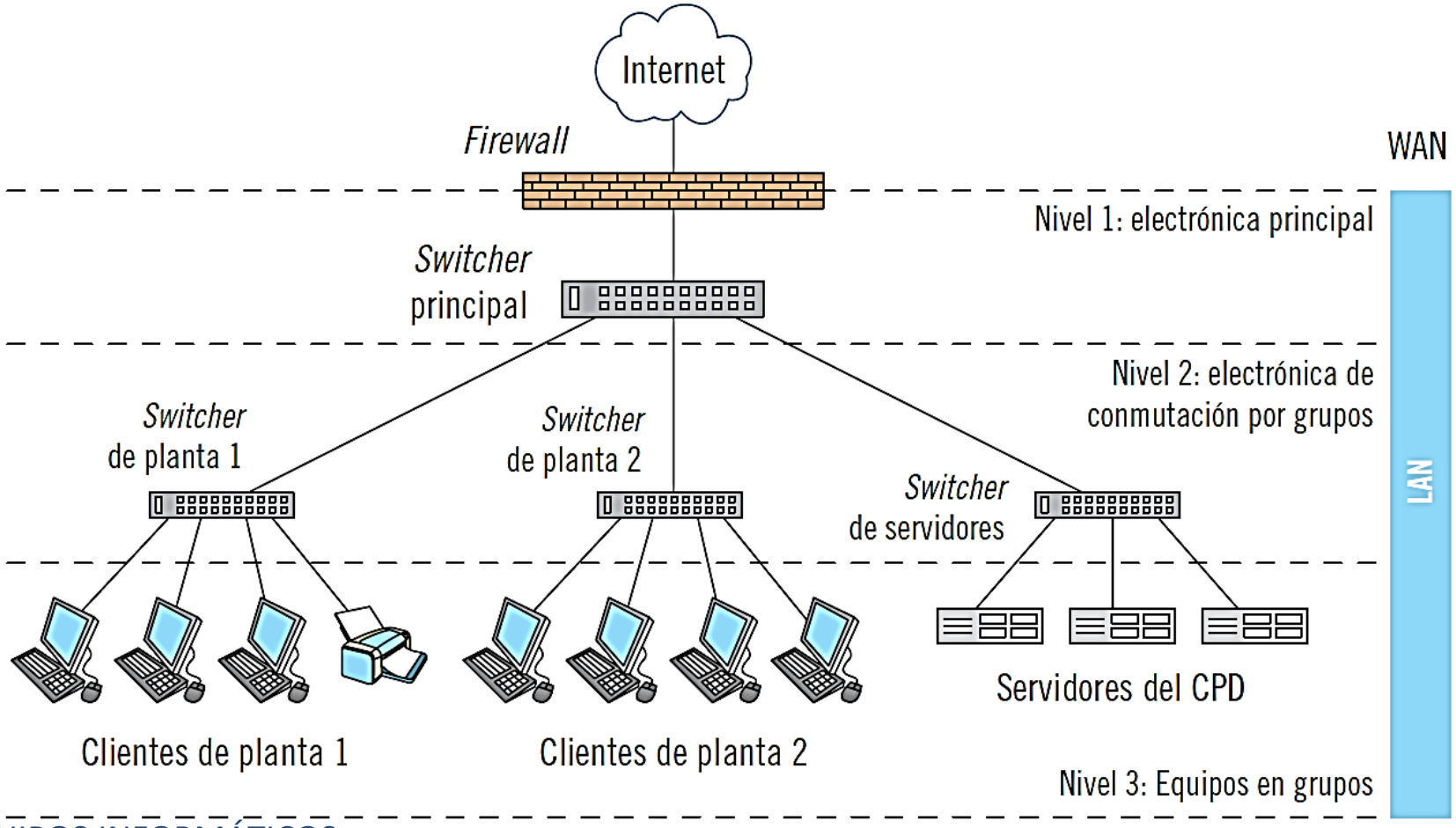
LOS **SERVIDORES** NORMALMENTE **SE UBICAN EN UN MISMO CPD**, POR LO QUE CONFLUYEN EN UN **SWITCH PARA SERVIDORES**, QUE IRÁ CONECTADO AL **SWITCH PRINCIPAL**.

PARA QUE TODOS LOS EQUIPOS TENGAN CONEXIÓN A INTERNET, EL **SWITCH PRINCIPAL SE CONECTA AL FIREWALL (O ROUTER),** Y ESTE ÚLTIMO, EN SU LADO PÚBLICO, **SE CONECTA A LA TOMA QUE ENTREGUE EL PROVEEDOR DE ACCESO**.

DE ESTA MANERA, **SE MANTIENE UNA ESTRUCTURA ORDENADA Y CONTROLADA**, QUE PERMITE GESTIONAR ADECUADAMENTE LAS COMUNICACIONES.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS



# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

ADEMÁS DEL CONTROL DE SEGREGACIÓN, ES NECESARIO INTERPONER **OTRAS MEDIDAS**. LA NORMA **ISO 27002** ESTABLECE EL OBJETIVO **CONTROLES DE RED**, PARA ASEGURAR LA PROTECCIÓN DE LA INFORMACIÓN EN LAS REDES Y LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN. MEDIANTE LAS SIGUIENTES **MEDIDAS**:

- DEBERÍAN ESTABLECERSE LAS **RESPONSABILIDADES Y LOS PROCEDIMIENTOS PARA LA GESTIÓN DE LOS EQUIPOS DE RED**.
- **LA RESPONSABILIDAD OPERACIONAL DE LAS REDES DEBERÍA ESTAR SEPARADA DE LAS OPERACIONES DE LOS SISTEMAS INFORMÁTICOS** DONDE SEA APROPIADO.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

- DEBERÍAN ESTABLECERSE **CONTROLES ESPECIALES PARA SALVAGUARDAR** LA CONFIDENCIALIDAD E INTEGRIDAD DE **LOS DATOS QUE PASAN A TRAVÉS DE REDES PÚBLICAS O DE REDES INALÁMBRICAS** Y PROTEGER LOS SISTEMAS CONECTADOS Y SUS APLICACIONES. TAMBIÉN PODRÍAN SER NECESARIOS **CONTROLES ESPECIALES PARA MANTENER LA DISPONIBILIDAD DE LOS SERVICIOS DE RED** Y LOS ORDENADORES CONECTADOS.
- DEBERÍA **REALIZARSE UN ADECUADO REGISTRO DE EVENTOS Y MONITORIZACIÓN** PARA PERMITIR EL REGISTRO Y DETECCIÓN DE ACCIONES QUE PODRÍAN AFECTAR, O SER RELEVANTES, PARA LA SEGURIDAD DE LA INFORMACIÓN.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

- **LAS ACTIVIDADES DE GESTIÓN DEBERÍAN ESTAR ESTRECHAMENTE COORDINADAS**, TANTO PARA OPTIMIZAR EL SERVICIO A LA ORGANIZACIÓN, COMO PARA ASEGURAR QUE LOS CONTROLES SEAN APLICADOS CONSISTENTEMENTE EN TODA LA INFRAESTRUCTURA DE TRATAMIENTO DE LA INFORMACIÓN.
- LOS **SISTEMAS DE LA RED** DEBERÍAN SER **AUTENTICADOS**.
- LA **CONEXIÓN DE LOS SISTEMAS A LA RED DEBERÍA SER RESTRINGIDA**.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

LAS MEDIDAS ANTERIORES DEBEN **LLEVARSE A LA PRÁCTICA SIEMPRE CON CRITERIO PROPORCIONAL.**

PARTIENDO DE **UNA ADECUADA DOCUMENTACIÓN DE LA RED**, SE DEBE **ANALIZAR CADA ELEMENTO**, PARA VER CUÁLES SON LAS MEDIDAS MÁS EFECTIVAS QUE PUEDEN APLICARSE.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## CIFRADO DE LAS COMUNICACIONES: IPSEC

ES UN **PROTOCOLO** DE LA CAPA DE INTERNET, **QUE APORTA SEGURIDAD AL PROTOCOLO IP**, AÑADIÉNDOLE POSIBILIDADES DE CIFRADO. AL OPERAR EN LA CAPA DE INTERNET, **APORTA SEGURIDAD A TODOS LOS PROTOCOLOS SUPERIORES**.

**IPSEC** SOPORTA DOS MODOS DE FUNCIONAMIENTO:

- **EL MODO TRANSPORTE,** ORIENTADO A COMUNICACIONES DE ORDENADOR A ORDENADOR, EN EL QUE SOLO SE CIFRA EL CONTENIDO DEL PAQUETE, Y LA CABECERA SE MANTIENE INTACTA COMO EN EL PROTOCOLO IP.
- **EL MODO TÚNEL,** ORIENTADO A COMUNICACIONES RED A RED, EN EL QUE SE CIFRA COMPLETAMENTE EL PAQUETE (INCLUIDA SU CABECERA) Y EL RESULTADO SE CONSIDERA COMO LA INFORMACIÓN ÚTIL DE UN NUEVO PAQUETE IP, QUE SE PROCESA NORMALMENTE.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## CARPETAS, IMPRESORAS Y OTROS RECURSOS

ADEMÁS DE LAS MEDIDAS DE PROTECCIÓN QUE SE PUEDEN APLICAR EN LA RED QUE DA ACCESO A LOS RECURSOS COMPARTIDOS, SE DEBERÍAN CONSIDERAR LAS SIGUIENTES **MEDIDAS ESPECÍFICAS REFERENTES A LAS IMPRESORAS**:

- SOLO DEBEN SER INSTALABLES POR USUARIOS CON PRIVILEGIOS PARA ELLO.
- LOS CONTROLADORES DE LAS IMPRESORAS DEBERÍAN GESTIONARSE SEGÚN UN PROCEDIMIENTO FORMAL.
- LAS IMPRESORAS NO DEBERÍAN TENER CONEXIÓN HACIA O DESDE INTERNET.
- LAS IMPRESORAS DEBERÍAN DISPONER DE UN SISTEMA DE CONTROL DE ACCESO, PARA CONTROLAR QUÉ USUARIOS TIENEN PERMISOS DE IMPRESIÓN.
- LAS IMPRESORAS DEBERÍAN TENER UN MODO DE IMPRESIÓN SEGURA.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## CARPETAS, IMPRESORAS Y OTROS RECURSOS

EN LO REFERENTE A LAS **CARPETAS COMPARTIDAS**, Y OTROS RECURSOS PARECIDOS, DEBEN APROVECHARSE LAS CAPACIDADES DE LOS SISTEMAS OPERATIVOS PARA **ESPECIFICAR PRIVILEGIOS A RECURSOS Y FICHEROS INDIVIDUALES**.

LOS ADMINISTRADORES DEBERÍAN **CONTROLAR EL ACCESO A LOS RECURSOS DEL SERVIDOR EN DOS ASPECTOS**: **CONTROLAR EL ACCESO DE LA APLICACIÓN**, Y **CONTROLAR EL ACCESO DE LOS USUARIOS**.

# 8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

## CARPETAS, IMPRESORAS Y OTROS RECURSOS

UN ADECUADO CUMPLIMIENTO DE LO ANTERIOR CONFIERE PROTECCIÓN PARA LOS ATAQUES DE DENEGACIÓN DE SERVICIO, ASÍ:

- **LAS CARPETAS** PARA COMPARTIR FICHEROS O APLICACIONES QUE REALICEN ESTA FUNCIÓN, DEBERÍAN **EMPLEAR DISCOS** DUROS O UNIDADES LÓGICAS **DIFERENTES A LOS EMPLEADOS POR EL SISTEMA OPERATIVO**
- SE PUEDEN EMPLEAR **SISTEMAS DE CUOTA DE DISCO** PARA LIMITAR EL ESPACIO QUE LOS USUARIOS PUEDEN CONSUMIR CARGANDO ARCHIVOS.

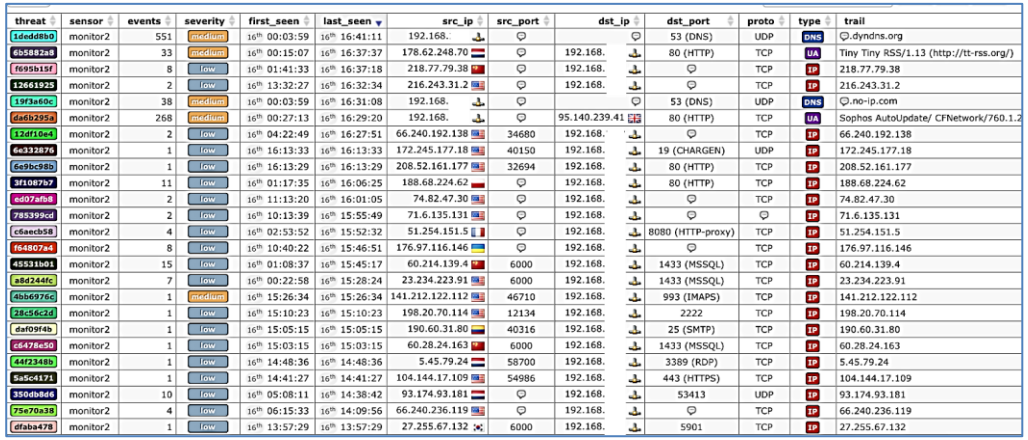
# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. **MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN**

# 9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

**LOS SISTEMAS DE INFORMACIÓN DEBEN MONITORIZARSE**, PARA **MEDIR LA EFICACIA DE LAS SALVAGUARDAS** QUE LOS PROTEGEN **Y OBTENER EVIDENCIAS** PARA VALORAR SI ESTAS SALVAGUARDAS SON NECESARIAS.

ADEMÁS, **LAS MEDIDAS DE SEGURIDAD** APLICADAS TENDRÁN VULNERABILIDADES, Y **PODRÍAN VERSE DESACTIVADAS O INUTILIZADAS**, PERMITIENDO QUE EL SISTEMA ESTÉ COMPROMETIDO SIN SABERLO.



| threat | sensor | events | severity | first_seen | last_seen | src_ip | src_port | dst_ip | dst_port | proto | type | trail |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1edd8b0 | monitor2 | 551 | medium | 16th 00:03:59 | 16th 16:41:11 | 192.168. | | | 53 (DNS) | UDP | DNS | dyndns.org |
| 6b5882a8 | monitor2 | 33 | medium | 16th 00:15:07 | 16th 16:37:37 | 178.62.248.70 | | 192.168. | 80 (HTTP) | TCP | UA | Tiny Tiny RSS/1.13 (http://tt-rss.org/) |
| f695b15f | monitor2 | 8 | low | 16th 01:41:33 | 16th 16:37:18 | 218.77.79.38 | | 192.168. | | TCP | IP | 218.77.79.38 |
| 12661925 | monitor2 | 2 | low | 16th 13:32:27 | 16th 16:32:34 | 216.243.31.2 | | 192.168. | | TCP | IP | 216.243.31.2 |
| 19f3a60c | monitor2 | 38 | medium | 16th 00:03:59 | 16th 16:31:08 | 192.168. | | | 53 (DNS) | UDP | DNS | no-ip.com |
| da6b295a | monitor2 | 268 | medium | 16th 00:27:13 | 16th 16:29:20 | 192.168. | | 95.140.239.41 | 80 (HTTP) | TCP | UA | Sophos AutoUpdate/ CFNetwork/760.1.2 |
| 12df10e4 | monitor2 | 2 | low | 16th 04:22:49 | 16th 16:27:51 | 66.240.192.138 | 34680 | 192.168. | | TCP | IP | 66.240.192.138 |
| 6e332876 | monitor2 | 1 | low | 16th 16:13:33 | 16th 16:13:33 | 172.245.177.18 | 40150 | 192.168. | 19 (CHARGEN) | UDP | IP | 172.245.177.18 |
| 6e9bc98b | monitor2 | 1 | low | 16th 16:13:29 | 16th 16:13:29 | 208.52.161.177 | 32694 | 192.168. | 80 (HTTP) | TCP | IP | 208.52.161.177 |
| 3f1087b7 | monitor2 | 11 | low | 16th 01:17:35 | 16th 16:06:25 | 188.68.224.62 | | 192.168. | 80 (HTTP) | TCP | IP | 188.68.224.62 |
| ed07afb8 | monitor2 | 2 | low | 16th 11:13:20 | 16th 16:01:05 | 74.82.47.30 | | 192.168. | | TCP | IP | 74.82.47.30 |
| 785399cd | monitor2 | 2 | low | 16th 10:13:39 | 16th 15:55:49 | 71.6.135.131 | | 192.168. | | | IP | 71.6.135.131 |
| c6aecb58 | monitor2 | 4 | low | 16th 02:53:52 | 16th 15:52:32 | 51.254.151.5 | | 192.168. | 8080 (HTTP-proxy) | TCP | IP | 51.254.151.5 |
| f64807a4 | monitor2 | 8 | low | 16th 10:40:22 | 16th 15:46:51 | 176.97.116.146 | | 192.168. | | TCP | IP | 176.97.116.146 |
| 45531b01 | monitor2 | 15 | low | 16th 01:08:37 | 16th 15:45:17 | 60.214.139.4 | 6000 | 192.168. | 1433 (MSSQL) | TCP | IP | 60.214.139.4 |
| a8d244fc | monitor2 | 7 | low | 16th 00:22:58 | 16th 15:28:24 | 23.234.223.91 | 6000 | 192.168. | 1433 (MSSQL) | TCP | IP | 23.234.223.91 |
| 4bb6976c | monitor2 | 1 | medium | 16th 15:26:34 | 16th 15:26:34 | 141.212.122.112 | 46710 | 192.168. | 993 (IMAPS) | TCP | IP | 141.212.122.112 |
| 28c56c2d | monitor2 | 1 | low | 16th 15:10:23 | 16th 15:10:23 | 198.20.70.114 | 12134 | 192.168. | 2222 | TCP | IP | 198.20.70.114 |
| daf09f4b | monitor2 | 1 | low | 16th 15:05:15 | 16th 15:05:15 | 190.60.31.80 | 40316 | 192.168. | 25 (SMTP) | TCP | IP | 190.60.31.80 |
| c6478e50 | monitor2 | 1 | low | 16th 15:03:15 | 16th 15:03:15 | 60.28.24.163 | 6000 | 192.168. | 1433 (MSSQL) | TCP | IP | 60.28.24.163 |
| 44f2348b | monitor2 | 1 | low | 16th 14:48:36 | 16th 14:48:36 | 5.45.79.24 | 58700 | 192.168. | 3389 (RDP) | TCP | IP | 5.45.79.24 |
| 5a5c4171 | monitor2 | 1 | low | 16th 14:41:27 | 16th 14:41:27 | 104.144.17.109 | 54986 | 192.168. | 443 (HTTPS) | TCP | IP | 104.144.17.109 |
| 350db8d6 | monitor2 | 10 | low | 16th 05:08:11 | 16th 14:38:42 | 93.174.93.181 | | 192.168. | 53413 | UDP | IP | 93.174.93.181 |
| 75e70a38 | monitor2 | 4 | low | 16th 06:15:33 | 16th 14:09:56 | 66.240.236.119 | | 192.168. | | TCP | IP | 66.240.236.119 |
| dfaba478 | monitor2 | 1 | low | 16th 13:57:29 | 16th 13:57:29 | 27.255.67.132 | 6000 | 192.168. | 5901 | TCP | IP | 27.255.67.132 |

# 9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## REGISTROS Y SUPERVISIÓN

LA NORMA **ISO 27002** ESTABLECE EL CONTROL **REGISTRO DE EVENTOS**, PARA REGISTRAR, PROTEGER Y REVISAR PERIÓDICAMENTE LAS ACTIVIDADES DE LOS USUARIOS, EXCEPCIONES, FALLOS Y EVENTOS DE SEGURIDAD DE LA INFORMACIÓN. **LOS REGISTROS DE EVENTOS DEBERÍAN INCLUIR**, CUANDO SEA RELEVANTE:

- IDENTIFICADORES (ID) DE USUARIO.
- ACTIVIDADES DEL SISTEMA.
- FECHAS, TIEMPOS Y DETALLES DE EVENTOS CLAVE, POR EJEMPLO, CONEXIÓN (LOG-ON) Y DESCONEXIÓN (LOG-OFF).
- IDENTIDAD O LOCALIZACIÓN DEL DISPOSITIVO, SI ES POSIBLE E IDENTIDAD DEL SISTEMA.

# 9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## REGISTROS Y SUPERVISIÓN

- REGISTRO DE INTENTOS DE ACCESO A LOS SISTEMAS EXITOSOS Y FALLIDOS.
- REGISTRO DE INTENTOS DE ACCESO A LOS RECURSOS Y A LOS DATOS EXITOSOS Y FALLIDOS.
- CAMBIOS EN LA CONFIGURACIÓN DEL SISTEMA.
- USO DE PRIVILEGIOS.
- USO DE UTILIDADES Y APLICACIONES DEL SISTEMA.
- FICHEROS A LOS QUE SE HA ACCEDIDO Y EL TIPO DE ACCESO.
- DIRECCIONES Y PROTOCOLOS DE RED.
- ALARMAS GENERADAS POR EL SISTEMA DE CONTROL DE ACCESO.
- ACTIVACIÓN Y DESACTIVACIÓN DE LOS SISTEMAS DE PROTECCIÓN, TALES COMO SISTEMAS DE ANTIVIRUS Y DE DETECCIÓN DE INTRUSIÓN.
- REGISTRO DE TRANSACCIONES EJECUTADAS POR USUARIOS EN LAS APLICACIONES.

# 9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## REGISTROS Y SUPERVISIÓN

EL CONTROL **PROTECCIÓN DE LA INFORMACIÓN DEL REGISTRO** INDICA QUE LOS **DISPOSITIVOS DE REGISTRO** Y LA **INFORMACIÓN DEL REGISTRO** DEBERÍAN **ESTAR PROTEGIDOS CONTRA MANIPULACIONES INDEBIDAS Y ACCESOS NO AUTORIZADOS**, INCLUYENDO:

- ALTERACIONES EN LOS TIPOS DE MENSAJES QUE SON REGISTRADOS.
- EDICIÓN O BORRADO DE LOS FICHEROS DE REGISTRO.
- SUPERACIÓN DE LA CAPACIDAD DE ALMACENAMIENTO DE LOS SOPORTES DE FICHEROS DE REGISTRO.

# 9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## REGISTROS Y SUPERVISIÓN

EL CONTROL **REGISTROS DE ADMINISTRACIÓN Y OPERACIÓN** INDICA QUE *SE DEBERÍAN REGISTRAR, PROTEGER Y REVISAR REGULARMENTE LAS ACTIVIDADES DEL ADMINISTRADOR DEL SISTEMA Y DEL OPERADOR DEL SISTEMA*.

POR ÚLTIMO, EL CONTROL **SINCRONIZACIÓN DEL RELOJ** INDICA *QUE LOS RELOJES DE TODOS LOS SISTEMAS DE TRATAMIENTO DE INFORMACIÓN* DENTRO DE UNA ORGANIZACIÓN O DE UN DOMINIO DE SEGURIDAD, *DEBERÍAN ESTAR SINCRONIZADOS CON UNA ÚNICA FUENTE DE TIEMPO* PRECISA Y ACORDADA.

# 9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

**ESTABLECER MEDIDAS ORGANIZATIVAS** QUE DICTEN CUÁLES SON LAS **CONDICIONES DE USO ADECUADO DE LOS SISTEMAS** DE INFORMACIÓN **AUMENTARÁ LA CONCIENCIA DE SEGURIDAD DE LOS USUARIOS**, Y REDUCIRÁ LA POSIBILIDAD DE INCIDENTES.

# 9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

NO SE DEBERÍA PODER ACCEDER A LOS RECURSOS PARA DESARROLLAR ACTIVIDADES QUE PERSIGAN O TENGAN COMO CONSECUENCIA:

- EL USO INTENSIVO DE RECURSOS DE PROCESO, MEMORIA, ALMACENAMIENTO O COMUNICACIONES, PARA USOS NO PROFESIONALES.
- LA DEGRADACIÓN DE LOS SERVICIOS.
- LA MODIFICACIÓN NO AUTORIZADA Y PREMEDITADA DE INFORMACIÓN.
- LA VIOLACIÓN DE LA INTIMIDAD, DEL SECRETO DE LAS COMUNICACIONES Y DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES.
- EL DETERIORO INTENCIONADO DEL TRABAJO DE OTRAS PERSONAS.
- EL USO DE LOS SISTEMAS DE INFORMACIÓN PARA FINES AJENOS A LOS DE LA ORGANIZACIÓN, SALVO EXCEPCIONES QUE SE CONTEMPLEN EXPRESAMENTE.
- DAÑAR INTENCIONADAMENTE LOS RECURSOS INFORMÁTICOS DE LA ORGANIZACIÓN O DE OTRAS INSTITUCIONES.
- INCURRIR EN CUALQUIER OTRA ACTIVIDAD ILÍCITA, DEL TIPO QUE SEA.

# CONTENIDOS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA QUE UTILICEN PROTOCOLOS SEGUROS DONDE SEA POSIBLE
6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

## RESUMEN

LOS SISTEMAS ESTÁN EXPUESTOS A MUCHAS AMENAZAS LÓGICAS, SIENDO CRÍTICO REDUCIR LAS DEBILIDADES EN LOS SERVIDORES QUE DAN SERVICIO A LOS ORDENADORES CLIENTE.

ESTO SE LLAMA **ROBUSTECIMIENTO** Y CONLLEVA ANALIZAR CADA SISTEMA, PORQUE LAS DEBILIDADES SERÁN DIFERENTES.

CUANTO MEJOR SE CONOZCA EL SISTEMA EN PRODUCCIÓN MENOS PROBABLE ES QUE AFECTE UNA AMENAZA, QUE SUELE APROVECHAR UN ERROR ESPECÍFICO, OCULTO Y CONCRETO DEL SISTEMA.

## RESUMEN

LOS FABRICANTES Y ENTIDADES COMO NIST Y CIS, OFRECEN GUÍAS QUE DEBEN SEGUIRSE PARA ROBUSTECER UN SISTEMA. LAS RECOMENDACIONES BÁSICAS SON:

- MODIFICAR LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DEL SISTEMA. ADEMÁS, NO SE DEBEN MANTENER ACTIVAS AQUELLAS CON IDENTIFICADOR ESTÁNDAR.
- CONFIGURAR LAS DIRECTIVAS DE CONTRASEÑAS, EN LONGITUD, COMPLEJIDAD, E HISTÓRICO SIN REPETICIÓN, PERIODO MÁXIMO Y MÍNIMO DE VIGENCIA, ADEMÁS DEL BLOQUEO POR INTENTOS DE ACCESO FALLIDOS.
- DESINSTALAR TODAS LAS APLICACIONES Y SERVICIOS INNECESARIOS, YA QUE LA SUPERFICIE DE ATAQUE DE UN SISTEMA ES MAYOR CUANTAS MÁS FUNCIONES DESEMPEÑE. SI ES POSIBLE, USAR SISTEMAS PARA FUNCIONES ÚNICAS.
- EMPLEAR SERVICIOS Y PROTOCOLOS SEGUROS, GENERALMENTE MEDIANTE SSL Y TLS, QUE AÑADEN TÉCNICAS DE CIFRADO PARA PROTEGER LAS COMUNICACIONES.

# RESUMEN

- MANTENERSE INFORMADO DE LAS VULNERABILIDADES DESCUBIERTAS, PARA APLICAR LOS PARCHES DE CORRECCIÓN Y SEGURIDAD QUE SE LIBEREN. EVITAR LA APLICACIÓN AUTOMÁTICA EN ENTORNOS DE PRODUCCIÓN SIN PROBARSE ANTES.
- PROTEGER LOS SISTEMAS DE CÓDIGO MALICIOSO CON PROGRAMAS ESPECÍFICOS, EN LAS CONEXIONES A INTERNET, Y DONDE SE USEN MEDIOS EXTRAÍBLES.
- GESTIÓN SEGURA DE LAS COMUNICACIONES, MEDIANTE SEPARACIÓN DE REDES, MEDIDAS DE SEGURIDAD EN LA ELECTRÓNICA DE RED, Y USO DE CORTAFUEGOS.
- MONITORIZAR LA SEGURIDAD, USAR LOS REGISTROS DE AUDITORÍA DEL SISTEMA CON HERRAMIENTAS DE ANÁLISIS Y ALERTA AUTOMÁTICO. EL USO CORRECTO DE LOS SISTEMAS DEBE PROMOVERSE ESPECIFICANDO USOS PROHIBIDOS.

ESTAS MEDIDAS DEBEN SER PROPORCIONALES AL RIESGO DE LOS SISTEMAS, PERO SIEMPRE DEBERÍA HABER UNA APLICACIÓN MÍNIMA DE LOS ASPECTOS SEÑALADOS.

# ESTO ES TODO