IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

RESUMEN

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN
3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES
4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES
5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

RESUMEN

LOS EQUIPOS INFORMÁTICOS SON CADA VEZ MÁS RELEVANTES PARA LA ACTIVIDAD DE LAS EMPRESAS, TANTO POR EL VALOR DE LA INFORMACIÓN QUE MANEJAN, COMO POR LAS CONSECUENCIAS DE LAS ACCIONES (U OMISIÓN DE LAS MISMAS), EN LAS QUE PARTICIPAN.

EXISTEN AMENAZAS DE TODO TIPO, SIEMPRE PRESENTES, QUE COMPROMETEN LA ACTIVIDAD DE LOS EQUIPOS, GRACIAS A **LAS VULNERABILIDADES** QUE LOS EQUIPOS PRESENTAN A ESTAS AMENAZAS.

NO PUDIENDO ELIMINARLAS POR COMPLETO, SE PUEDE AFIRMAR QUE NO EXISTE LA SEGURIDAD “CERO”.

RESUMEN

SIN EMBARGO, SI **SE PUEDE REDUCIR** EL DAÑO PROBABLE QUE UNA AMENAZA TENDRÍA EN UN EQUIPO, ES DECIR, **EL RIESGO** QUE EL EQUIPO ENTRAÑA PARA LA EMPRESA.

EL **RIESGO ES MAYOR CUANTO MAYOR SEA EL** DAÑO O **IMPACTO** QUE UNA AMENAZA CAUSARÍA EN UN EQUIPO, **Y** CUANTO MAYOR SEA **LA PROBABILIDAD** DE OCURRENCIA DE LA AMENAZA.

ES POSIBLE **REDUCIR ESTE RIESGO**, O BIEN REDUCIENDO EL DAÑO QUE CAUSARÍA UNA AMENAZA, **O REDUCIENDO LA PROBABILIDAD** DE QUE ESTA SE APLIQUE SOBRE UNA VULNERABILIDAD DEL SISTEMA, ES DECIR, REDUCIENDO LAS DEBILIDADES DEL EQUIPO.

RESUMEN

EL DAÑO, HABITUALMENTE, **SE EVALÚA** EN TODAS LAS **DIMENSIONES O PROPIEDADES DE LA INFORMACIÓN**, QUE EN EL ÁMBITO DE LA SEGURIDAD DE LA INFORMACIÓN SON TRES:

LA CONFIDENCIALIDAD, LA INTEGRIDAD, Y LA DISPONIBILIDAD

ES DECIR, LA INFORMACIÓN ES SEGURA SI SE PUEDA ACCEDER A ELLA CUANDO SE NECESITA (**DISPONIBILIDAD**), SOLO POR QUIEN LO NECESITA **(CONFIDENCIALIDAD**), Y SI ES VÁLIDA, PORQUE SOLO LA HA MODIFICADO QUIEN PUEDE HACERLO (**INTEGRIDAD**).

RESUMEN

PARA GESTIONAR LA SEGURIDAD, SE EMPLEA UN MODELO DE **GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN EL RIESGO**, Y QUE CONSTA DE **DOS FASES**:

- EN UNA **PRIMERA FASE**, EL **ANÁLISIS DE RIESGOS**, SE ANALIZA EL RIESGO DE LAS AMENAZAS SOBRE LOS EQUIPOS INFORMÁTICOS.
- EN UNA **SEGUNDA FASE**, LA **GESTIÓN DE RIESGOS,** SE EVALÚA SI ESE RIESGO SE PUEDE ASUMIR O NO, DE ACUERDO CON UNAS NORMAS INTERNAS, O LEYES QUE AFECTEN A LA EMPRESA.

EN CASO DE QUE NO SE PUEDA ASUMIR, HAY QUE **REDUCIRLO**, **INTRODUCIENDO** PARA ELLO LAS **SALVAGUARDAS** O MEDIDAS ADECUADAS.

RESUMEN

ES MUY FRECUENTE EMPLEAR **UN CRITERIO DE COSTE/BENEFICIO, O DE ANÁLISIS DE VIABILIDAD EN TÉRMINOS ECONÓMICOS PARA DETERMINAR LA ADECUACIÓN DE UNA SALVAGUARDA**. BASTARÍA COMPARAR EL COSTE DE LA SALVAGUARDA CON EL COSTE DEL RIESGO, PARA PRESENTAR LA DECISIÓN DE VIABILIDAD A LA DIRECCIÓN.

ESTABLECIDA ESTA METODOLOGÍA GENERAL**, SE DEBE PROFUNDIZAR EN CONOCER LOS RIESGOS** MÁS HABITUALES DE UN EQUIPO INFORMÁTICO **Y**, POR LO TANTO, **LAS POSIBLES SALVAGUARDAS**.

LOS RIESGOS SON DE NATURALEZA AMBIENTAL O DEL ENTORNO, DERIVADOS DEL ACCESO FÍSICO, O DERIVADOS DEL ACCESO LÓGICO A LOS EQUIPOS.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN
3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO
4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD

RESUMEN

EL OBJETIVO DE UN SGSI ES ASEGURAR LA CONTINUIDAD DEL NEGOCIO, MINIMIZANDO LOS RIESGOS Y MAXIMIZANDO EL RETORNO DE LA INVERSIÓN EN SEGURIDAD. PARA ELLO**, HAY QUE CONOCER LOS RIESGOS MEDIANTE UN PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS.**

ESTE ANÁLISIS PUEDE EMPLEARSE COMO PUNTO DE PARTIDA PARA REALIZAR EL **BIA**, O **ANÁLISIS DEL IMPACTO EN EL NEGOCIO** QUE TENDRÍA UN INCIDENTE DE SEGURIDAD QUE DETUVIERA LA ACTIVIDAD.

EL **BIA** SE PUEDE **REALIZAR MEDIANTE** LA PROPIA INFORMACIÓN QUE SE RECOJA EN **FORMULARIOS**, Y QUE PERMITIRÁ DETERMINAR CUÁLES SON LOS PROCESOS O FUNCIONES PRINCIPALES DE LA EMPRESA DONDE FOCALIZAR LOS ESFUERZOS EN LAS SALVAGUARDAS.

RESUMEN

EL RESULTADO DE UN BIA ES MUY VALIOSO, PORQUE **PERMITE CONOCER LA ACTIVIDAD DE LA EMPRESA**, **ORDENANDO LA CRITICIDAD** DE SUS FUNCIONES Y PROCESOS.

TAMBIÉN PERMITE **CONOCER EL COSTE DE UNA INTERRUPCIÓN**, Y RECOGE LOS REQUISITOS DE PUNTO OBJETIVO DE RECUPERACIÓN.

EL **BIA** AYUDA A **DETERMINAR LAS ESTRATEGIAS O MÉTODOS DE RECUPERACIÓN**, **Y LAS SALVAGUARDAS** O CONTRAMEDIDAS QUE SE APLICARÍAN.

LOS REQUISITOS DE SEGURIDAD SERÁN CALIFICACIONES, NÚMEROS, O GRADOS, ALCANZADOS EN CADA UNA DE LAS DIMENSIONES DE LA SEGURIDAD (**LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD**).

RESUMEN

LOS REQUISITOS DE SEGURIDAD DEL PROCESO DE NEGOCIO PUEDEN OBTENERSE EVALUANDO LOS REQUISITOS DE LA INFORMACIÓN RESULTANTE DEL PROCESO O ANALIZANDO LOS COMPONENTES DEL PROCESO, Y **VALORANDO LOS REQUISITOS DE SEGURIDAD DE CADA COMPONENTE**.

UNA VEZ DISPUESTOS JERÁRQUICAMENTE, **LOS REQUISITOS DE SEGURIDAD SE AGRUPAN DE MANERA ASCENDENTE**, MEDIANTE ALGUNA FÓRMULA O MÉTODO DEFINIDO (INDICADOR).

RESUMEN

ESTOS INDICADORES PERSIGUEN COMPARAR LA EVOLUCIÓN DE LA EMPRESA EN DIFERENTES INSTANTES DEL TIEMPO.

POR LO TANTO**, LO IMPORTANTE ES QUE ESTOS CRITERIOS SE DEFINAN POR ESCRITO, Y SE APLIQUEN CON HOMOGENEIDAD A LO LARGO DEL SGSI**, PORQUE SOLO ASÍ SE PODRÁ RECONOCER LA TENDENCIA DE MEJORA EN LA SEGURIDAD OBTENIDA POR CADA ITERACIÓN DEL MISMO (PLANIFICACIÓN, EJECUCIÓN, MEDIDA, Y CORRECCIÓN).

CONTENIDOS

1. INTRODUCCIÓN
2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES
3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS
4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RESUMEN

LA INVERSIÓN DE ESFUERZO **EN SEGURIDAD DE LA INFORMACIÓN** DEBE REALIZARSE SEGÚN **UN MÉTODO DE ANÁLISIS Y GESTIÓN DE RIESGOS**.

MAGERIT ES UNA NORMA ESPAÑOLA, QUE CUMPLE PERFECTAMENTE ESTE COMETIDO, Y CUYO ANÁLISIS **CONSTA DE 5 PASOS**:

- EVALUACIÓN DE ACTIVOS **(1)**
- EVALUACIÓN DE AMENAZAS **(2)** EN TÉRMINOS DE LA DEGRADACIÓN
- CALCULAR EL IMPACTO **(4)**
- FRECUENCIA QUE DETERMINE EL RIESGO **(5)**
- EL PASO **(3)** ES CONSIDERAR LAS CONTRAMEDIDAS, Y SE REALIZA HABITUALMENTE DESPUÉS, PARA MEDIR LA MEJORA QUE APORTAN.

RESUMEN

LO IMPORTANTE, ES QUE **LOS CRITERIOS** APLICADOS **SE PONGAN POR ESCRITO**, **Y SE APLIQUEN DE MANERA HOMOGÉNEA** ENTRE SISTEMAS Y ANUALIDADES DEL AGR.

MAGERIT APORTA UNA **CLASIFICACIÓN DE LOS ACTIVOS**, Y UNA METODOLOGÍA PARA ORDENAR SUS DEPENDENCIAS JERÁRQUICAS, E INTRODUCE LOS CONCEPTOS DE IMPACTO ACUMULADO Y REPERCUTIDO, Y DE RIESGO ACUMULADO Y REPERCUTIDO.

TAMBIÉN APORTA UN **CATÁLOGO DE AMENAZAS**, INCLUIDA LA NATURALEZA DEL ACTIVO AFECTADO, Y LA PRIORIDAD DE LA DIMENSIÓN DE SEGURIDAD AFECTADA.

RESUMEN

TRAS EL ANÁLISIS DEL RIESGO RESIDUAL, SE DEBE GESTIONAR, MITIGÁNDOLO, EVITÁNDOLO, TRANSFIRIÉNDOLO, O ACEPTÁNDOLO.

SI LA OPCIÓN ES MITIGAR, SE ELIGEN **CONTRAMEDIDAS** SEGÚN SU EFECTO EN LA REDUCCIÓN DEL RIESGO, DEBIENDO SER PRIORITARIAMENTE **PREVENTIVAS, DE DETECCIÓN, Y REACTIVAS** (PRIMERO DE EMERGENCIA, Y DESPUÉS DE RECUPERACIÓN).

EN LA EVALUACIÓN ECONÓMICA, SE PERSEGUIRÁ EL **EQUILIBRIO ENTRE EL COSTE DE LA SEGURIDAD, Y EL COSTE DE LA INSEGURIDAD**.

RESUMEN

PARA LA APLICACIÓN DE SALVAGUARDAS, **MAGERIT** PROPONE UN **PROCEDIMIENTO ORDENADO**, QUE EXIGE:

- UNA **POLÍTICA** ORGANIZATIVA,
- UNOS **OBJETIVOS** DEFINIDOS PARA SABER SI EL RIESGO SE LOGRA REDUCIR
- UNAS **INSTRUCCIONES** PASO A PASO DE CÓMO PONER EN MARCHA LAS SALVAGUARDAS ELEGIDAS, PARA A CONTINUACIÓN APLICARLAS Y EVALUAR SU EFICACIA.

CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO
3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

RESUMEN

LA INTERVENCIÓN EN **SI** PASA PRIMERO POR **ANALIZAR LOS REQUISITOS** QUE DEBE TENER LA EMPRESA.

LOS CRITERIOS PARA ESTO SON L**AS LEYES, LAS NORMAS, LOS OBJETIVOS, Y LA RENTABILIDAD.**

ESTOS CRITERIOS SUBYACEN EN LAS 3 FUENTES DE INFORMACIÓN QUE SE USAN PARA ACOTAR ESTOS REQUISITOS: UN **AGR**, EL CONJUNTO DE **REGULACIÓN Y NORMATIVA** QUE SE DEBE CUMPLIR, Y **LOS OBJETIVOS** (INCLUIDOS LOS COMERCIALES), QUE EL SISTEMA DE INFORMACIÓN DEBA CUMPLIR PARA SOSTENER LAS OPERACIONES.

RESUMEN

ESTA LABOR NO ES SENCILLA, Y **DEBEN DEDICARSE RECURSOS PROPORCIONALES, Y UN ENFOQUE CONSTRUCTIVO DE MEJORA REITERADA**.

LOS REQUISITOS PUEDEN SER **EN UNA O EN TODAS LAS DIMENSIONES CIA**, Y PUEDEN **FIJARSE PARA EL PROCESO MÁS CRÍTICO, PARA DOS, O PARA TODOS.**

LOS REQUISITOS PUEDEN INCLUIR UNA LISTA DE CHEQUEO DE RESULTADOS O CONTROLES ESPECÍFICOS PARA LA EMPRESA. UNA VEZ DETERMINADO EL PERFIL DE **SI** REQUERIDO, PROCEDE CONOCER DE QUÉ SITUACIÓN PARTE LA EMPRESA.

AQUÍ SE TRATA DE EVALUAR EL **SI** DE LA EMPRESA, Y NUEVAMENTE, NO ES TAREA SENCILLA RESUMIRLO EN UN NÚMERO O UNA PALABRA..

RESUMEN

LAS HERRAMIENTAS SON LOS **INFORMES DE AUDITORÍAS BASADAS EN RIESGO** QUE PUEDAN EXISTIR (Y QUE INCLUIRÁN UN AR QUE EXPRESE EL RIESGO RESIDUAL), UN **REGISTRO DE INCIDENTES DE SEGURIDAD** DEBIDAMENTE ENTENDIDO E INTERPRETADO, LAS **MEDICIONES DE EFECTIVIDAD DE LOS CONTROLES IMPLANTADAS**, Y **LAS OPINIONES O RECOMENDACIONES DE LOS INTERESADOS**, QUE PUEDAN SER RELEVANTES

LA **DIFERENCIA ENTRE REQUISITOS DESEADOS Y GRADO DE CUMPLIMIENTO** DE LOS MISMOS ES LA **MEJORA O DIFERENCIA** QUE SE DEBE LOGRAR.

PARA ELLO, SE APLICARÁN UNAS **CONTRAMEDIDAS** DIRIGIDAS A TENER MAYORES NIVELES CIA, QUE LOGRE QUE SE RESPONDA POSITIVAMENTE A TODAS LAS PREGUNTAS DE UNA LISTA DE CHEQUEO.

RESUMEN

LA SELECCIÓN DE ESTAS MEDIDAS ES UN TRABAJO DE DISEÑO, DONDE APLICAN CRITERIOS GENERALES Y OTROS ESPECÍFICOS DE **PÉRDIDAS Y GANANCIAS**.

SIEMPRE, ANTE LA DUDA, PUEDEN EMPLEARSE UN CONJUNTO DE **MEDIDAS MÍNIMAS**, O **LÍNEA BASE DE PARTIDA**.

PARA LA APLICACIÓN DE ESTE CONJUNTO DE SALVAGUARDAS MÍNIMO, U OTROS QUE SE DECIDAN AÑADIR, EL TRABAJO DEBE ORDENARSE EN TORNO A UN PLAN DE IMPLANTACIÓN. ESTE DOCUMENTO TIENE COMPONENTES COMUNES PARA LA ÓPTICA DE **ISO 27002**, O PARA LA PERSPECTIVA **MAGERIT.**

RESUMEN

SE TRATA DE ESTABLECER, PRIMERO, UN **MARCO DE REFERENCIA** Y UN **CONJUNTO DE PLANES DE ACCIÓN**, QUE AGRUPEN LOS PAQUETES DE SALVAGUARDAS O MEDIDAS A IMPLANTAR.

PARA CADA PROGRAMA O **PLAN DE ACCIÓN**, DEBE DARSE: **UNA DESCRIPCIÓN Y OBJETIVO, UNA PRIORIDAD, UN PERIODO DE EJECUCIÓN, UNOS RECURSOS, UNAS TAREAS A REALIZAR, EL DETALLE DE LA FINANCIACIÓN, UNOS RESPONSABLES, Y UNA MEDIDA DE LA EFICACIA**, QUE AFECTE A UNO O VARIOS DE LOS CONTROLES A IMPLANTAR.

CONTENIDOS

1. INTRODUCCIÓN
2. PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES. SUJETOS IMPLICADOS EN LA PROTECCIÓN DE LOS DATOS
3. DERECHOS DE LAS PERSONAS Y DERECHOS DIGITALES
4. TRATAMIENTOS CONCRETOS Y TRANSFERENCIAS A TERCEROS PAÍSES Y ORGANIZACIONES INTERNACIONALES
5. VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS. INFRACCIONES Y SANCIONES

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 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.

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**.

ES PRIMORDIAL **ASEGURAR EL SUMINISTRO ELÉCTRICO**, LOS SERVICIOS DE PROTECCIÓN CONTRA INCENDIOS Y LA CLIMATIZACIÓN.

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.

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**.

RESUMEN

A SU VEZ, LA **INFORMACIÓN DE LOS USUARIOS** SE GESTIONA MEDIANTE **SERVICIOS DE DIRECTORIO**.

EL **REGISTRO Y MONITORIZACIÓN DE SUCESOS** ES UNA HERRAMIENTA FUNDAMENTAL.

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**.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN
3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS
4. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

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

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.

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

CONTENIDOS

1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

RESUMEN

INTERNET ES LA PRINCIPAL FUENTE DE AMENAZAS PARA LA RED DE LA EMPRESA, Y A LA VEZ, RESULTA IMPRESCINDIBLE.

POR TANTO, SE DEBE REDUCIR EN LO POSIBLE ESTA VULNERABILIDAD, PRIMERO, MANTENIENDO CONTROLADOS Y DEFINIDOS LOS PUNTOS DE INTERCONEXIÓN Y, EN SEGUNDO LUGAR, EMPLEANDO EN DICHOS PUNTOS PASARELAS DE SEGURIDAD GENERALMENTE CONOCIDAS COMO **CORTAFUEGOS O FIREWALLS**.

POR SU FUNCIONAMIENTO, SON HABITUALES EL EMPLEO DE **FIREWALLS DE FILTRADO DE PAQUETES** (DE MANERA ESTÁTICA O DE MANERA DINÁMICA), O BIEN **FIREWALLS DE APLICACIÓN**, FORMADOS POR SERVIDORES PROXY QUE INTERRUMPEN LA COMUNICACIÓN ENTRE CLIENTES Y SERVIDORES A MODO DE BUFFER, O APLICACIÓN INTERMEDIA.

RESUMEN

POR SU CONSTRUCCIÓN, SE PUEDEN ENCONTRAR DISEÑOS QUE VAN DESDE UN SENCILLO ROUTER PROPORCIONADO POR EL ISP, HASTA SUBREDES FILTRADAS QUE PERMITEN LA EXISTENCIA DE ZONAS INTERMEDIAS (**ZONAS DESMILITARIZADA, DMZ**), DONDE GENERALMENTE SE DEBEN UBICAR LOS SERVIDORES QUE TENGAN QUE SER ACCEDIDOS DESDE EL EXTERIOR, O SUS REEMPLAZOS (ES DECIR **SERVIDORES PROXY** PARA EL ACCESO EXTERNO); SIN OLVIDAR LOS **FIREWALLS PERSONALES**, QUE SE UBICAN EN CADA CLIENTE DE LA RED PRIVADA.

EL EMPLEO DE FIREWALLS PROTEGE EL PERÍMETRO, CONTROLANDO EL ACCESO A LA RED PRIVADA DESDE INTERNET, Y VICEVERSA.

PESE A ELLO, PERSISTE EL PROBLEMA DEL ACCESO A LA INFORMACIÓN, CUANDO ESTA CIRCULA LIBREMENTE POR INTERNET, O CUANDO CIRCULA POR LA RED PRIVADA, SI EL ATAQUE PROCEDE DE LA PROPIA RED PRIVADA.

RESUMEN

PARA ELLO, SE EMPLEAN **REDES PRIVADAS VIRTUALES**, QUE CONSTITUYEN CONEXIONES (**TÚNELES**) SEGUROS ENTRE EMISOR Y RECEPTOR, GRACIAS AL EMPLEO DE AUTENTICACIÓN Y ENCRIPTACIÓN.

ENTRE LOS PROTOCOLOS VPN MÁS USADOS, DESTACAN **PPTP** Y **L2TP**, FUNCIONANDO EN CAPA 2, E **IPSEC**, FUNCIONANDO EN CAPA 3.

EL USO CONJUNTO DE FIREWALLS Y VPN, PARA SEPARAR LA LAN DE INTERNET O PARA SEPARAR SUBREDES LAN O DOMINIOS LÓGICOS DE SEGURIDAD INTERNOS, COMPLETAN LAS SALVAGUARDAS QUE PERMITEN CERRAR PERFECTAMENTE LA INFRAESTRUCTURA (FÍSICA Y LÓGICA) EN TORNO A LOS ACTIVOS CONTENIDOS.

COMO OTRAS CONTRAMEDIDAS, SE DEBE MONITORIZAR SU EFICACIA Y RENDIMIENTO MEDIANTE REGISTROS DE AUDITORÍA Y VERIFICACIONES REGULARES DE SU BUEN FUNCIONAMIENTO, DESCONFIANDO DEL COMPORTAMIENTO CONOCIDO

ACTIVIDADES

- ACTIVIDAD 01. CONFIGURACIÓN DE SEGURIDAD WINDOWS
- ACTIVIDAD 02. PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA
- ACTIVIDAD 03. AMENAZAS, VULNERABILIDADES E INCIDENTES DE SEGURIDAD INFORMÁTICA
- ACTIVIDAD 04. USO DE POWERSHELL
- ACTIVIDAD 05. LAS CERTIFICACIONES TIER
- ACTIVIDAD 06. SEGURIDAD EN REDES SOCIALES
- ACTIVIDAD 07. DIRECCIONAMIENTO DE RED Y SUBREDES
- ACTIVIDAD 08. LA CONTINUIDAD DEL NEGOCIO
- ACTIVIDAD 09. REQUISITOS CIA DE UN PROCESO, DIRECCIONAMIENTO IP Y MÁQUINA LINUX (E1)

ACTIVIDADES

- ACTIVIDAD 10. ISO 27002-2022
- ACTIVIDAD 11. VISUAL STUDIO CODE
- ACTIVIDAD 12. DETERMINACIÓN DE COSTES DE UN INCIDENTE
- ACTIVIDAD 13. CONFIGURACIÓN DE SEGURIDAD LINUX
- ACTIVIDAD 14. LENGUAJE PYTHON
- ACTIVIDAD 15. APLICACIÓN DE MAGERIT (EN CLASE)
- ACTIVIDAD 16. PLAN DE SEGURIDAD
- ACTIVIDAD 17. PLAN DE SEGURIDAD INFORMÁTICA Y COSTES DE UN INCIDENTE (E2)
- ACTIVIDAD 18. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DERECHOS DIGITALES

ACTIVIDADES

- ACTIVIDAD 19. PROTECCIÓN CONTRA LA PUBLICIDAD. LA LISTA ROBINSON
- ACTIVIDAD 20. HERRAMIENTAS DE BÚSQUEDA EN LINUX, CMD Y POWERSHELL
- ACTIVIDAD 21. USO DE EXPRESIONES REGULARES
- ACTIVIDAD 22. ROBUSTECIMIENTO DE SISTEMAS
- ACTIVIDAD 23.IMPLANTACIÓN DE UN CPD PARA UNA ORGANIZACIÓN (E3)

ANEXOS

- CONFIGURACIÓN DE SEGURIDAD WINDOWS
- CONCEPTOS DE SEGURIDAD INFORMÁTICA
- POWERSHELL
- LAS CERTIFICACIONES TIER
- LA CONTINUIDAD DE NEGOCIO
- INSTALACIÓN LINUX DEBIAN SIN MODO GRÁFICO
- ISO 27002-2022
- GESTIÓN DE RIESGOS
- INSTALACIÓN DE EDITOR DE CÓDIGO VISUAL STUDIO CODE
- CONFIGURACIÓN DE SEGURIDAD LINUX
- LENGUAJE PYTHON

ANEXOS

- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
- PLAN DE SEGURIDAD INFORMÁTICA
- MAGERIT
- PLAN DE CONTINUIDAD DEL NEGOCIO
- ROBUSTECIMIENTO DE SISTEMAS

ESTO ES TODO