IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UD01

CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

OBJETIVOS DEL MÓDULO

- ANALIZAR LOS PLANES DE IMPLANTACIÓN DE LA ORGANIZACIÓN PARA IDENTIFICAR LOS ELEMENTOS DEL SISTEMA IMPLICADOS Y LOS NIVELES DE SEGURIDAD A IMPLEMENTAR.
- ANALIZAR E IMPLEMENTAR LOS MECANISMOS DE ACCESO FÍSICOS Y LÓGICOS A LOS SERVIDORES SEGÚN ESPECIFICACIONES DE SEGURIDAD.
- EVALUAR LA FUNCIÓN Y NECESIDAD DE CADA SERVICIO EN EJECUCIÓN EN EL SERVIDOR SEGÚN LAS ESPECIFICACIONES DE SEGURIDAD.
- INSTALAR, CONFIGURAR Y ADMINISTRAR UN CORTAFUEGOS DE SERVIDOR CON LAS CARACTERÍSTICAS NECESARIAS SEGÚN ESPECIFICACIONES DE SEGURIDAD.

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

1. INTRODUCCIÓN

EL USO DE EQUIPOS INFORMÁTICOS SE HA AMPLIADO A LA TOTALIDAD DE ORGANIZACIONES.

ACTUALMENTE ACTÚAN DE FORMA MUY IMPORTANTE EN LA REALIZACIÓN DE SERVICIOS Y ENTREGA DE PRODUCTOS DE UNA EMPRESA.

EN ALGUNOS CASOS, **LOS EQUIPOS INFORMÁTICOS MANEJAN INFORMACIÓN IMPORTANTE**, COMO DATOS FINANCIEROS, O DATOS DE CARÁCTER ESTRATÉGICO.

1. INTRODUCCIÓN

EN OTROS CASOS, **LOS EQUIPOS REALIZAN ACCIONES DIRECTAMENTE.** POR EJEMPLO, EN LOS PROCESOS PRODUCTIVOS DIRIGEN MÁQUINAS.

EN EMPRESAS DE LOGÍSTICA Y TRANSPORTE DE MERCANCÍAS, **TOMAN DECISIONES MEDIANTE REGLAS PROGRAMADAS**, Y DATOS PROCEDENTES DE SENSORES.

INCLUSO **INTERVIENEN EN LA EJECUCIÓN DE ÓRDENES EN SISTEMAS DE SOPORTE VITAL HUMANO**, COMO EN HOSPITALES Y LABORATORIOS.

1. INTRODUCCIÓN

LOS EQUIPOS INFORMÁTICOS I**NTERVIENEN TAMBIÉN EN INFRAESTRUCTURAS CRÍTICAS**, COMO PLANTAS DE PRODUCCIÓN Y DISTRIBUCIÓN ELÉCTRICA, CENTRALES NUCLEARES, SISTEMAS DE TRANSPORTE AÉREO O FERROVIARIO, INFRAESTRUCTURAS DE TELECOMUNICACIONES, O EN SISTEMAS DE DEFENSA.

1. INTRODUCCIÓN

ACTUANDO SOBRE ESTOS EQUIPOS INFORMÁTICOS, SE PUEDEN ALTERAR O BORRAR DATOS, INCLUSO MODIFICAR PRODUCTOS Y SERVICIOS EN LOS QUE INTERVIENEN.

EXISTE UNA CRECIENTE **NECESIDAD** ACTUAL DE **EMPLEAR MECANISMOS Y TÉCNICAS DE PROTECCIÓN FRENTE A POSIBLES AMENAZAS EN LOS EQUIPOS INFORMÁTICOS**, PARA DEFENDER LOS PRODUCTOS Y SERVICIOS DE LA EMPRESA

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

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

ES NECESARIO PROTEGER LOS EQUIPOS INFORMÁTICOS. VEREMOS QUÉ ELEMENTOS INTERVIENEN EN UN PROBLEMA DE SEGURIDAD (**AMENAZA, VULNERABILIDAD E INCIDENTE DE SEGURIDAD**).

HAREMOS UNA CLASIFICACIÓN DE LOS ASPECTOS A PROTEGER, O **PRINCIPIOS DE SEGURIDAD**, Y DEL MÉTODO PARA FIJAR DICHA PROTECCIÓN, BASÁNDONOS EN EL RIESGO DE UN INCIDENTE.

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

LA SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS CUBRE ESTA NECESIDAD DE PROTECCIÓN, OBJETIVO QUE **COMPARTE CON DISCIPLINAS** SIMILARES COMO LA **SEGURIDAD INFORMÁTICA, LA SEGURIDAD DE LA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (TIC), Y LA SEGURIDAD DE LA INFORMACIÓN.**

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

VEAMOS DOS **DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN**, QUE ENGLOBAN TAMBIÉN A LOS EQUIPOS INFORMÁTICOS:

- **ISO 27000**
- **MAGERIT**

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

ISO 27000

LA SEGURIDAD DE LA INFORMACIÓN ES **LA PRESERVACIÓN DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN**.

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

MAGERIT

LA METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (**MAGERIT**) DEL MINISTERIO DE ADMINISTRACIONES PÚBLICAS, EN , DEFINE SEGURIDAD COMO:

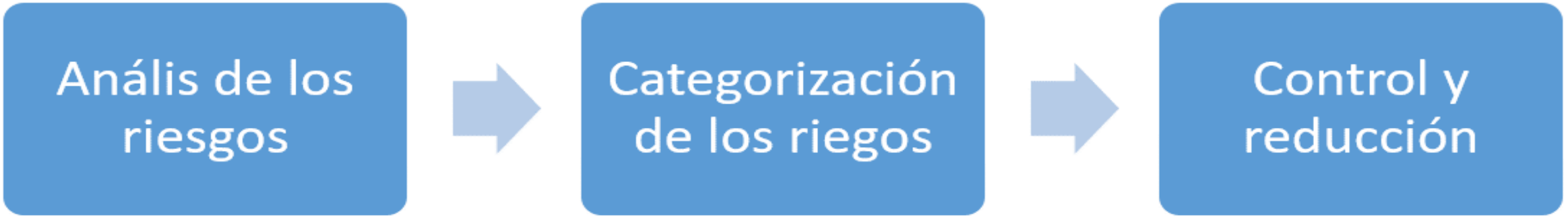
LA CAPACIDAD DE LAS REDES O DE LOS SISTEMAS DE INFORMACIÓN, DE RESISTIR, CON UN DETERMINADO NIVEL DE CONFIANZA, LOS ACCIDENTES O ACCIONES ILÍCITAS O MALINTENCIONADAS QUE COMPROMETAN LA DISPONIBILIDAD, AUTENTICIDAD, INTEGRIDAD Y CONFIDENCIALIDAD DE LOS DATOS ALMACENADOS O TRANSMITIDOS, Y DE LOS SERVICIOS QUE DICHAS REDES Y SISTEMAS OFRECEN O HACEN ACCESIBLES.

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

LA FINALIDAD DE LA **GESTIÓN DEL RIESGO** ES:

REALIZAR UN ANÁLISIS PARA PODER DETERMINAR Y REALIZAR UNA VALORACIÓN OBJETIVA ACERCA DE LOS RIESGOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN Y APLICAR MECANISMOS QUE PERMITAN CONTROLARLO

PARA SU DESARROLLO ***SE DEFINEN TRES FASES***:



2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

ANÁLISIS DE LOS RIESGOS

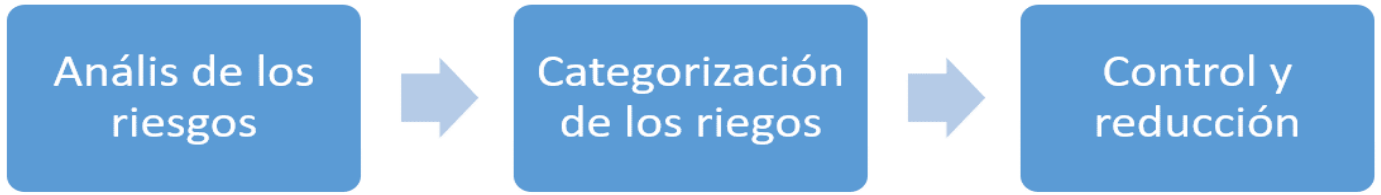
SE REALIZAN PRUEBAS PARA VALORAR LA VULNERABILIDAD DE CADA UNO DE LOS SISTEMAS.

CATEGORIZACIÓN DE LOS RIESGOS

SE ASIGNAN CATEGORÍAS A LOS RIESGOS Y SE CLASIFICAN PARA PODER VALORARLOS.

CONTROL Y REDUCCIÓN

SE REALIZAN LAS ACCIONES NECESARIAS PARA CONTROLAR Y REDUCIR AL MÍNIMO EL IMPACTO DE LAS AMENAZAS.



2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.1 AMENAZAS, VULNERABILIDADES E INCIDENTES DE SEGURIDAD

EN PRIMER LUGAR, VAMOS A DEFINIR LOS CONCEPTOS DE **AMENAZA, VULNERABILIDAD E INCIDENTE DE SEGURIDAD**.

AMENAZA

LAS **AMENAZAS** *SON* ***LAS POSIBLES ACCIONES QUE DAÑARÍAN LOS EQUIPOS INFORMÁTICOS***. LAS AMENAZAS NO SE PUEDEN ELIMINAR, POR LO TANTO, EXISTE LA OBLIGACIÓN DE ANALIZARLAS PARA PODER REDUCIR EL DAÑO QUE SUPONDRÍAN EN LOS EQUIPOS INFORMÁTICOS

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.1 AMENAZAS, VULNERABILIDADES E INCIDENTES DE SEGURIDAD

VULNERABILIDAD

LAS **VULNERABILIDADES** SON ***LAS DEBILIDADES DE LOS EQUIPOS ANTE LAS AMENAZAS***. LA VULNERABILIDAD FACILITA QUE UNA AMENAZA DAÑE EL EQUIPO

INCIDENTE DE SEGURIDAD

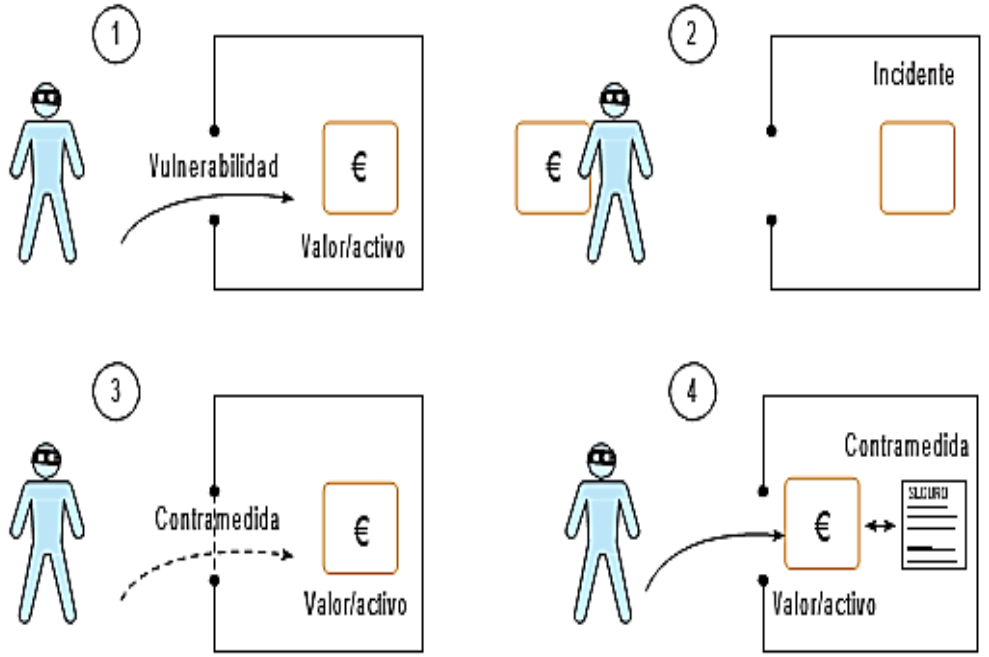
CUANDO UNA AMENAZA SUCEDE Y APROVECHA UNA VULNERABILIDAD SE DICE QUE HA OCURRIDO UN **INCIDENTE DE SEGURIDAD**

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.1 AMENAZAS, VULNERABILIDADES E INCIDENTES DE SEGURIDAD

LAS AMENAZAS SERÁN GENÉRICAS, MIENTRAS ***QUE LAS VULNERABILIDADES SERÁN PARTICULARES DE CADA EQUIPO***, Y SÍ SE PUEDE INTERVENIR SOBRE ELLAS.

FRENTE A LOS INCIDENTES DE SEGURIDAD, DEBEMOS DISPONER DE **CONTRAMEDIDAS** PARA CONOCER, PREVENIR, IMPEDIR, REDUCIR Y CONTROLAR EL DAÑO QUE PODRÍA TENER UN EQUIPO.



2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.1 AMENAZAS, VULNERABILIDADES E INCIDENTES DE SEGURIDAD

DEBEMOS SIEMPRE PONERNOS EN EL PEOR DE LOS CASOS:

TARDE O TEMPRANO EL INCIDENTE DE SEGURIDAD SE VA A PRODUCIR

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.1 AMENAZAS, VULNERABILIDADES E INCIDENTES DE SEGURIDAD

EL TRABAJO DE SEGURIDAD CONSISTE EN:

- **REDUCIR LA FRECUENCIA** CON LA QUE OCURRAN LOS INCIDENTES
- **REDUCIR EL DAÑO** CUANDO ESTOS SE PRODUZCAN

ES **EN LAS CONTRAMEDIDAS DONDE SE CENTRARÁ LA ATENCIÓN Y EL TRABAJO PRÁCTICO**, BUSCANDO LA FORMA MÁS EFECTIVA PARA **REDUCIR LA PROBABILIDAD DE OCURRENCIA Y LOS DAÑOS DE UN INCIDENTE**, Y MAXIMIZANDO ASÍ LA RELACIÓN BENEFICIO/COSTE.

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.2 PRINCIPIOS DE SEGURIDAD

DEBIDO A QUE LAS AMENAZAS NO SE PUEDEN ELIMINAR, SIEMPRE EXISTIRÁ ALGUNA VULNERABILIDAD QUE SE PODRÁ EXPLOTAR.

NO EXISTE LA SEGURIDAD TOTAL

LA SEGURIDAD PRETENDE QUE LOS SISTEMAS Y EQUIPOS DE INFORMACIÓN SEAN FIABLES. LA FIABILIDAD O SEGURIDAD, SE APOYA EN **TRES PRINCIPIOS DE SEGURIDAD**:

LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.2 PRINCIPIOS DE SEGURIDAD

CONFIDENCIALIDAD. QUE LA INFORMACIÓN SOLO ESTÉ ACCESIBLE PARA QUIEN ESTÉ AUTORIZADO A ELLO

INTEGRIDAD.QUE LA INFORMACIÓN SEA EXACTA Y COMPLETA, DE MANERA QUE SOLO PUEDA MODIFICARLA QUIEN ESTÉ AUTORIZADO A ELLO

DISPONIBILIDAD. QUE LA INFORMACIÓN ESTÉ ACCESIBLE CUANDO SEA NECESARIO

SE CONOCE COMO **LA TRÍADA CIA (CONFIDENTIALITY, INTEGRITY, AVAILABILITY)** Y SON LOS PRINCIPIOS BÁSICOS DE LA SEGURIDAD DE LA INFORMACIÓN

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.3 RIESGO DE UN INCIDENTE DE SEGURIDAD

EL RIESGO ES EL VALOR DEL DAÑO QUE CAUSARÍA UNA AMENAZA, APROVECHANDO UNA VULNERABILIDAD:

RIESGO = PROBABILIDAD X IMPACTO

SERÁ MAYOR CUANTO MÁS PROBABLE SEA LA AMENAZA, Y CUANTO MAYOR SEA EL DAÑO QUE PRODUZCA.

CUANTAS MÁS CONTRAMEDIDAS SE DISPONGAN, MENOR SERÁ EL DAÑO PROBABLE, O LO QUE ES LO MISMO, MENOR ES EL RIESGO PARA EL SISTEMA DE INFORMACIÓN.

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.3 RIESGO DE UN INCIDENTE DE SEGURIDAD

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.3 RIESGO DE UN INCIDENTE DE SEGURIDAD

***DEBE EXISTIR UN BALANCE ENTRE EL RIESGO DE UN INCIDENTE DE SEGURIDAD Y LOS RECURSOS QUE SE DEDIQUEN A REDUCIR SU DAÑO PROBABLE*.**

ESTE BALANCE DEBE SER GESTIONADO DE UNA FORMA METÓDICA POR VARIAS RAZONES:

- PARA PODER **ANALIZAR LA VIABILIDAD** DE LA INVERSIÓN EN SEGURIDAD
- PARA PODER **ANALIZAR LA MEJORA O NO**, EN EL CUMPLIMIENTO DE LOS OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN A LO LARGO DEL TIEMPO

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.3 RIESGO DE UN INCIDENTE DE SEGURIDAD

ESTE MÉTODO SISTEMÁTICO, SE DENOMINA:

MODELO DE SEGURIDAD

Y PERSIGUE ORGANIZAR LOS PROCESOS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, EN BASE A UNAS DIRECTRICES, Y ALGÚN MÉTODO PARA CALCULAR LOS RIESGOS DEL SISTEMA DE INFORMACIÓN.

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.3 RIESGO DE UN INCIDENTE DE SEGURIDAD

EN RESUMEN:

UN MODELO DE SEGURIDAD ORIENTADO A LA GESTIÓN DEL RIESGO, EMPLEA EL CÁLCULO DEL RIESGO, Y UNOS CRITERIOS EMPRESARIALES PARA PODER DECIDIR SI ES VIABLE REDUCIR EL RIESGO QUE SE ASUME, O NO.

2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN

2.3 RIESGO DE UN INCIDENTE DE SEGURIDAD

PARA ESTUDIAR EL RIESGO, *SE DEBEN SEGUIR DOS PASOS:*

- **EL ANÁLISIS DE RIESGOS:** CONSISTE EN *IDENTIFICAR AMENAZAS*, *DETERMINAR LAS VULNERABILIDADES*, Y *MEDIR EL IMPACTO* O DAÑO QUE CAUSARÍA UN INCIDENTE.
- **LA GESTIÓN DE RIESGOS:** PARTIENDO DE LOS RESULTADOS DEL ANÁLISIS DE RIESGOS, PERMITE *ELEGIR LAS CONTRAMEDIDAS* DE SEGURIDAD QUE SE IMPLANTARÁN.

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

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

HAY QUE TENER EN CUENTA QUE **CUANDO UN EQUIPO SE CONECTA A UNA RED ENTRA EN CONTACTO CON OTROS EQUIPOS** Y **EXISTE UN ALTO RIESGO DE ROBO DE INFORMACIÓN Y GENERAR UNA VULNERABILIDAD EN EL SISTEMA.**

AUNQUE EL EQUIPO NO ESTÉ CONECTADO A UNA RED NO ES GARANTÍA SUFICIENTE DE QUE NO ESTEMOS EN RIESGO Y PODAMOS RECIBIR UN ATAQUE.

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

LAS AMENAZAS A LAS QUE ESTÁ EXPUESTO UN SISTEMA DE INFORMACIÓN SON MUY DIVERSAS, POR LO QUE, **EN LA FASE INICIAL DE LA GESTIÓN DE RIESGOS, CONVIENE CENTRARSE EN LAS PRINCIPALES.**

POSTERIORMENTE, SE PODRÁ MEJORAR EL MODELO, AUMENTANDO EL CATÁLOGO DE AMENAZAS.

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

LAS AMENAZAS PUEDEN CLASIFICARSE COMO:

- **NATURALES O ARTIFICIALES**
- **DEBIDAS AL ENTORNO O AL HOMBRE**
- **ACCIDENTALES O INTENCIONADAS**

VEAMOS UN CONJUNTO DE AMENAZAS FRECUENTES, *EXTRAÍDO DEL CATÁLOGO DE AMENAZAS DE* ***MAGERIT***, ASÍ COMO ALGUNOS DE LOS RIESGOS PRINCIPALES, Y SALVAGUARDAS USUALES.

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

DESASTRES NATURALES

Amenaza	Riesgos usuales	Salvaguardas usuales
Incendios	Que el fuego acabe con recursos del sistema	Protección de las instalaciones frente a incendios
Inundaciones	Que el agua acabe con recursos del sistema	Protección de las instalaciones frente a inundaciones
Rayo, tormenta eléctrica	Destrucción de sistemas electrónicos	Protección de las instalaciones frente a descargas eléctricas

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

DE ORIGEN INDUSTRIAL

Amenaza	Riesgos usuales	Salvaguardas usuales
Incendios	Que el fuego acabe con recursos del sistema	Protección de las instalaciones frente a incendios
Inundaciones, escapes	Que el agua acabe con recursos del sistema	Protección de las instalaciones frente a inundaciones
Otros desastres industriales: sobrecarga eléctrica, fluctuaciones eléctricas	Destrucción de sistemas electrónicos	Protección de las instalaciones frente a descargas eléctricas

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

DE ORIGEN INDUSTRIAL

Amenaza	Riesgos usuales	Salvaguardas usuales
Contaminación mecánica: vibraciones, polvo, suciedad	Destrucción de sistemas electromecánicos	Mantenimiento preventivo de limpieza, y reposición de componentes electromecánicos
Avería de origen físico o lógico: fallos en los equipos, fallos en los programas	Paradas de sistemas y/o pérdida de trazabilidad	Disponer de sistemas de funcionamiento redundante
Corte del suministro eléctrico	Paradas de sistemas	Sistemas de alimentación ininterrumpida

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

DE ORIGEN INDUSTRIAL

Amenaza	Riesgos usuales	Salvaguardas usuales
Condiciones inadecuadas de temperatura y humedad	Destrucción de componentes	Sistemas de aire acondicionado, y alarma por exceso de temperatura y humedad
Fallo de servicios de comunicaciones	Parada de sistema	Disponer rutas de comunicación redundantes
Degradación de los soportes de almacenamiento	Paradas de sistemas y/o pérdida de trazabilidad	Empleo de soportes redundantes, y realización de copias de seguridad

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

ERRORES Y FALLOS NO INTENCIONADOS

Amenaza	Riesgos usuales	Salvaguardas usuales
Errores de los usuarios	Pérdida de información	Copias de seguridad, incluidos registros de transacciones para deshacer operaciones
Errores del administrador	Parada de sistema, ausencia de seguridad y trazabilidad	Disociación de responsabilidades, para reducir daño de los errores
Errores de configuración	Parada de sistema, ausencia de seguridad y trazabilidad	Procedimientos de reinstalación y configuración del sistema. Copias de seguridad

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

ERRORES Y FALLOS NO INTENCIONADOS

Amenaza	Riesgos usuales	Salvaguardas usuales
Deficiencias en la organización: cuando no está claro quién es responsable de hacer qué y cuándo	Paradas de sistemas, causadas por acciones descoordinadas u omisiones	Políticas de seguridad con establecimiento de responsables
Difusión de software dañino (virus, spyware, gusanos, troyanos, bombas lógicas, etc.)	Parada de sistema, ausencia de seguridad y trazabilidad	Software de eliminación de virus, y de eliminación de software malicioso. Procedimientos de reinstalación y configuración del sistema. Copias de seguridad
Escapes de información: la información llega a quien no debe	Perdida completa de confidencialidad	Uso de técnicas de encriptación

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

ERRORES Y FALLOS NO INTENCIONADOS

Amenaza	Riesgos usuales	Salvaguardas usuales
Alteración de la información: alteración accidental de la información	Pérdida completa de integridad	Sistemas de revisión y validación de transacciones (mediante totales, revisión por otra persona u otras vías)
Vulnerabilidades de los programas (defectos en el código que producen errores)	Paradas del sistema y/o perdida de integridad	Entornos de prueba y sistemas de revisión
Errores de mantenimiento o actualización de programas (software)	Paradas del sistema	Plan de mantenimiento preventivo, para revisar fecha de actualización aplicada a las aplicaciones

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

ERRORES Y FALLOS NO INTENCIONADOS

Amenaza	Riesgos usuales	Salvaguardas usuales
Caída del sistema por agotamiento de recursos	Paradas del sistema	Aplicaciones de monitorización de recursos disponibles con alarmas
Indisponibilidad del personal: ausencia accidental del puesto de trabajo por enfermedad, alteraciones de orden público, guerra, etc.	Paradas del sistema	Política de seguridad con establecimiento de responsables, y designación de suplentes de responsables

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

ATAQUES INTENCIONADOS

Amenaza	Riesgos usuales	Salvaguardas usuales
Manipulación de la configuración	Parada de sistema, ausencia de seguridad y trazabilidad	Copias impresas de procedimientos de reinstalación, y configuración del sistema
Suplantación de la identidad del usuario	Pérdida completa de confidencialidad e integridad	Sistemas de autenticación fuertes, que incluyan medidas biométricas
Uso no previsto: típicamente en interés personal, juegos, etc.	Paradas del sistema	Impedir ejecución de procesos no autorizados

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

ATAQUES INTENCIONADOS

Amenaza	Riesgos usuales	Salvaguardas usuales
Difusión de software dañino: virus, spyware, gusanos, troyanos, bombas lógicas, etc.	Parada de sistema, ausencia de seguridad y trazabilidad	Software de eliminación de virus y de eliminación de software malicioso. Procedimientos de reinstalación y configuración del sistema. Copias de seguridad
Análisis de tráfico	Conocimiento de las pautas de actividad de la empresa	Aleatorización de las rutas de comunicaciones, y encapsulamiento de protocolos
Repudio	Pérdida de trazabilidad de las operaciones	Empleo de firmas digitales

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

ATAQUES INTENCIONADOS

Amenaza	Riesgos usuales	Salvaguardas usuales
Interceptación de información (escucha)	Pérdida de confidencialidad	Empleo de técnicas de criptografía
Destrucción de la información	Paradas de sistema	Copias de seguridad
Divulgación de la información	Pérdida de confidencialidad	Empleo de técnicas de criptografía
Denegación de servicio	Paradas de sistema	Penalización a solicitudes recurrentes. Monitorización de recursos disponibles y alarma

3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES

ATAQUES INTENCIONADOS

Amenaza	Riesgos usuales	Salvaguardas usuales
Robo de equipos o soportes	Paradas de sistema y perdida de confidencialidad	Alarmas antirrobo, sistemas de anclaje de equipos, técnicas de criptografía
Ataque destructivo (vandalismo, terrorismo, etc.)	Paradas de sistema	Copias de seguridad fuera de las instalaciones, acuerdos de alquiler de equipos para casos de emergencia, copias impresas de procedimientos de reinstalación y configuración del sistema
Ingeniería social	Parada de sistema, ausencia de seguridad y trazabilidad	Formación, empleo de mecanismos de autenticación fuertes con métodos biométricos

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

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

LAS SALVAGUARDAS, O CONTRAMEDIDAS, SON ELEMENTOS DE DEFENSA, PARA QUE LAS AMENAZAS NO CAUSEN TANTO DAÑO. SE PUEDEN CLASIFICAR EN:

- **PREVENTIVAS O PROACTIVAS**
- **REACTIVAS**
- **DE "NO HACER NADA"**

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

PREVENTIVAS O PROACTIVAS

PERSIGUEN ANTICIPARSE A LA OCURRENCIA DEL INCIDENTE.

EJEMPLO: USO DE CONTRASEÑAS

REACTIVAS

PERSIGUEN REDUCIR EL DAÑO UNA VEZ OCURRE EL INCIDENTE.

EJEMPLO: LAS COPIAS DE SEGURIDAD

DE "NO HACER NADA"

ACEPTAR EL RIESGO EXISTENTE PARA LOS EQUIPOS.

EJEMPLO: UNA EMPRESA, CUYA POLÍTICA DE SEGURIDAD ESTABLECE QUE SE APROBARÁN LOS RIESGOS, CUANDO SEAN INFERIORES AL 10 % DEL VALOR DE LOS ACTIVOS.

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

VEAMOS ALGUNAS ÁREAS DE SEGURIDAD ESPECÍFICAS, CON SUS TECNOLOGÍAS HABITUALES Y SALVAGUARDAS:

- **SEGURIDAD DE RECURSOS HUMANOS**
- **SEGURIDAD AMBIENTAL**
- **SEGURIDAD FÍSICA**
- **SEGURIDAD DE ACCESO LÓGICO**

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD DE RECURSOS HUMANOS

TANTO **ANTES DEL EMPLEO, COMO DURANTE EL EMPLEO, Y A LA TERMINACIÓN DEL MISMO**, CONVIENE ADOPTAR MEDIDAS, SALVAGUARDAS, O CONTROLES, PARA PROTEGER LA INFORMACIÓN QUE SERÁ ACCEDIDA, E IMPACTADA POR LAS PERSONAS.

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD DE RECURSOS HUMANOS

DEPENDIENDO DE CADA CIRCUNSTANCIA, PODRÍA CORRESPONDER APLICAR ALGUNA DE LAS SIGUIENTES **SALVAGUARDAS HABITUALES**:

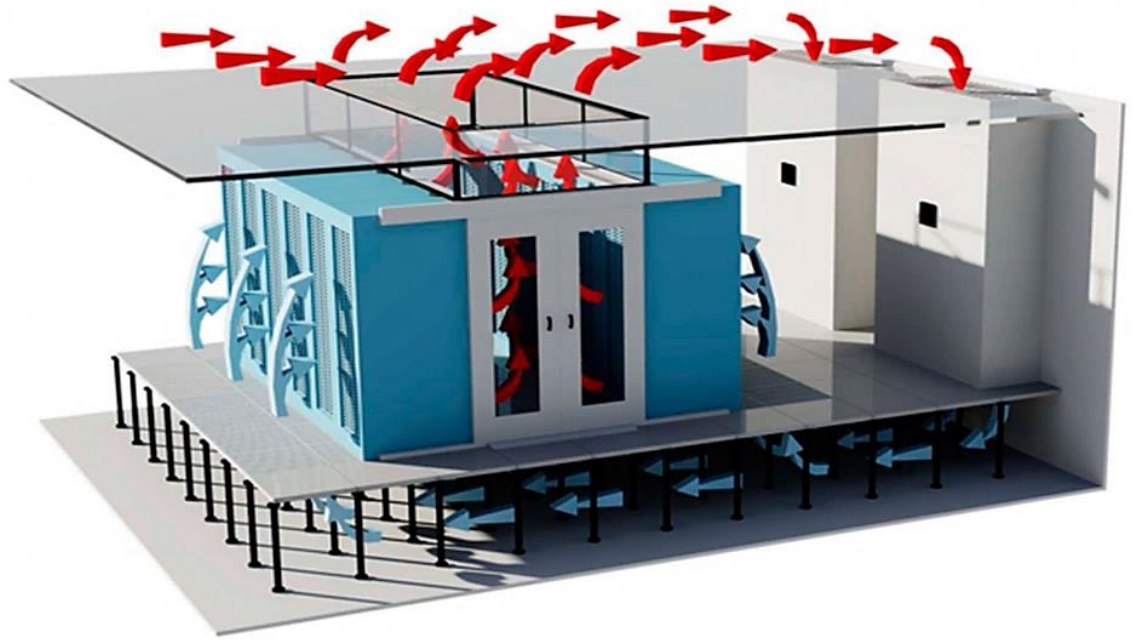
- DEFINICIÓN DE ROLES Y RESPONSABILIDADES QUE CONTRAERÁ EL TRABAJADOR.
- INVESTIGACIÓN DE ANTECEDENTES.
- FORMACIÓN Y CAPACITACIÓN DE LOS TRABAJADORES EN SEGURIDAD DE LA INFORMACIÓN.
- DEFINICIÓN DE PROCESOS DISCIPLINARIOS.
- DEFINIR LAS RESPONSABILIDADES A LA TERMINACIÓN DEL CONTRATO.
- DEVOLUCIÓN DE ACTIVOS.
- RETIRADA DE DERECHOS DE ACCESO A LA INFORMACIÓN.

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD AMBIENTAL

LOS EQUIPOS INFORMÁTICOS DEBEN **DISPONER DE UN ENTORNO ADECUADO**.

POR EJEMPLO, LAS CONDICIONES **DE TEMPERATURA Y SUMINISTRO ELÉCTRICO** DE LOS ORDENADORES DE LOS USUARIOS.



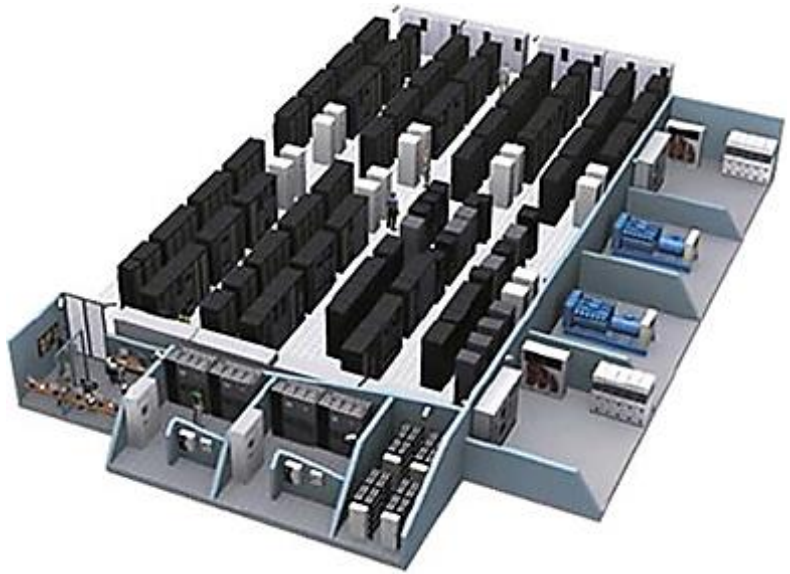
4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD AMBIENTAL

AL **SERVIDOR** HAY QUE PROPORCIONARLE UN ESPACIO MEJOR, PORQUE **EL RIESGO DE UNA AMENAZA ACTUANDO SOBRE ÉL ES MAYOR**:

DEBE PROPORCIONARSE UN SISTEMA DE ALIMENTACIÓN ELÉCTRICA ININTERRUMPIDO, Y UNAS CONDICIONES DE TEMPERATURA ADECUADAS.

DEBE INTENTAR UBICARSE EN UN RECINTO SEPARADO, CENTRO DE PROCESO DE DATOS O CPD.



4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD AMBIENTAL

LAS **SALVAGUARDAS MÁS HABITUALES** SON:

- MEDIDAS QUE EVITEN EL FUEGO, EL HUMO O EL AGUA.
- MEDIDAS QUE EVITEN LAS VIBRACIONES, GOLPES, Y CAÍDAS ACCIDENTALES.
- MEDIDAS PARA PROPORCIONAR TEMPERATURA Y HUMEDAD ADECUADAS.
- MEDIDAS QUE EVITEN FALLOS DE SUMINISTRO ELÉCTRICO.
- SEGURIDAD DEL CABLEADO.
- UN MANTENIMIENTO PREVENTIVO DE LOS EQUIPOS.
- ASEGURAR CONDICIONES DE SEGURIDAD PARA DESPLAZAMIENTOS DEL EQUIPO FUERA DEL CPD.
- SEGURIDAD AL FINAL DEL CICLO DE VIDA DEL EQUIPO, INCLUIDA SU DESTRUCCIÓN SEGURA.

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD FÍSICA

EL **ACCESO FÍSICO A LOS ORDENADORES** Y EQUIPOS **AUMENTA EL RIESGO** DE CUALQUIER INCIDENTE.

DEBE APLICARSE EL CRITERIO DE **CONCEDER ACCESO EXCLUSIVAMENTE A QUIEN LO NECESITE** POR SUS FUNCIONES Y SOLAMENTE CUÁNDO Y CÓMO LO NECESITA.

ASÍ, **LOS USUARIOS NO DEBEN TENER ACCESO FÍSICO A SERVIDORES, O A EQUIPOS DE COMUNICACIONES**.

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD FÍSICA

ENTRE LOS **INFRACTORES** SE PUEDEN ENCONTRAR *LOS PROPIOS USUARIOS O TRABAJADORES DE LA EMPRESA, ANTIGUOS EMPLEADOS QUE CONSERVEN SISTEMAS DE ACREDITACIÓN QUE LES DEN ACCESO, Y PERSONAS EXTERNAS, COMO LADRONES, SALTEADORES, O HACKERS*.

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD FÍSICA

SE TRATA DE **PROTEGER A LOS EQUIPOS** DE ACCIDENTES QUE OCURREN **CUANDO HAY ACCESO HUMANO** A LOS MISMOS.

SALVAGUARDAS MÁS HABITUALES PARA PROTEGER ACCESO FÍSICO SON:

- ESTABLECER UN PERÍMETRO DE SEGURIDAD FÍSICA
- MECANISMOS DE CONTROL DE INGRESO FÍSICO
- ESTABLECER Y DEFINIR ÁREAS DE ACCESO PÚBLICO, DE ENTREGA, DE CARGA, ETC.
- PROTECCIÓN CONTRA LOCALES O ACTIVIDADES CERCANAS

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD DE ACCESO LÓGICO

EL ACCESO LÓGICO **SE REFIERE AL ACCESO A LA INFORMACIÓN DE MANERA REMOTA**, ES DECIR, EN UNA RED DE COMUNICACIONES, QUE EXTIENDE EL ACCESO AL SERVIDOR MÁS ALLÁ DEL CPD.

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD DE ACCESO LÓGICO

LAS SALVAGUARDAS MÁS HABITUALES SON LAS SIGUIENTES:

- DEFINIR UNA POLÍTICA DE CONTROL DE ACCESO
- EXISTENCIA DE UN REGISTRO DE USUARIOS, Y DE LOS SERVICIOS A LOS QUE ACCEDEN
- GESTIÓN DE PRIVILEGIOS DE ACCESO
- GESTIÓN DE CLAVES DE USUARIO
- REVISIONES PERIÓDICAS DE LOS DERECHOS DE ACCESO DE LOS USUARIOS
- EL ESTABLECIMIENTO DE RESPONSABILIDADES DEL USUARIO
- LA EXISTENCIA DE UNA POLÍTICA DE USO DE LOS SERVICIOS DE RED
- MECANISMOS DE AUTENTICACIÓN Y REGISTRO PARA LAS CONEXIONES REMOTAS

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD DE ACCESO LÓGICO

- SEPARACIONES DE REDES
- CONTROLES DE LAS CONEXIONES QUE REALIZAN LOS USUARIOS HACIA FUERA DE LA EMPRESA
- CONTROLES DE ACCESO AL SISTEMA OPERATIVO
- CONTROLES DE ACCESO A LAS APLICACIONES Y LA INFORMACIÓN
- ESTABLECIMIENTO DE UNA POLÍTICA PARA TRABAJO EN MOVILIDAD

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD DE ACCESO LÓGICO

LAS SALVAGUARDAS MÁS HABITUALES SON LAS SIGUIENTES:

- DEFINIR UNA POLÍTICA DE CONTROL DE ACCESO.
- EXISTENCIA DE UN REGISTRO DE USUARIOS, Y DE LOS SERVICIOS A LOS QUE ACCEDEN.
- GESTIÓN DE PRIVILEGIOS DE ACCESO.
- GESTIÓN DE CLAVES DE USUARIO.
- REVISIONES PERIÓDICAS DE LOS DERECHOS DE ACCESO DE LOS USUARIOS.
- EL ESTABLECIMIENTO DE RESPONSABILIDADES DEL USUARIO.

4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES

SEGURIDAD DE ACCESO LÓGICO

- LA EXISTENCIA DE UNA POLÍTICA DE USO DE LOS SERVICIOS DE RED.
- MECANISMOS DE AUTENTICACIÓN Y REGISTRO PARA LAS CONEXIONES REMOTAS.
- SEPARACIONES DE REDES.
- CONTROLES DE LAS CONEXIONES QUE REALIZAN LOS USUARIOS HACIA FUERA DE LA EMPRESA.
- CONTROLES DE ACCESO AL SISTEMA OPERATIVO.
- CONTROLES DE ACCESO A LAS APLICACIONES Y LA INFORMACIÓN.
- ESTABLECIMIENTO DE UNA POLÍTICA PARA TRABAJO EN MOVILIDAD.

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**

5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

A LA VISTA DE LA MULTITUD DE AMENAZAS Y SALVAGUARDAS CONSIDERADAS **ES NECESARIA UNA GESTIÓN ADECUADA** DE ESAS MEDIDAS, QUE INCLUIRÁ:

LOS PROCESOS, REVISIONES, RECALIFICACIONES, Y ADAPTACIONES PARA LA REALIDAD CAMBIANTE DE LA EMPRESA, SU ENTORNO, SUS AMENAZAS Y SUS DEBILIDADES.

5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

PARA LA CONSTRUCCIÓN DE UN SISTEMA DE SEGURIDAD, **NO BASTAN LOS CONCEPTOS TECNOLÓGICOS, SINO QUE SE NECESITAN TAMBIÉN ASPECTOS DE GESTIÓN, ASPECTOS LEGALES, ASPECTOS ÉTICOS, U OTROS ESPECÍFICOS DE LA NATURALEZA Y AMBIENTE INTERNO Y EXTERNO DE LA EMPRESA.**

5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

SURGE ENTONCES EL CONCEPTO DE:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

COMO UN SISTEMA DE GESTIÓN USADO PARA ESTABLECER Y MANTENER UN ENTORNO SEGURO.

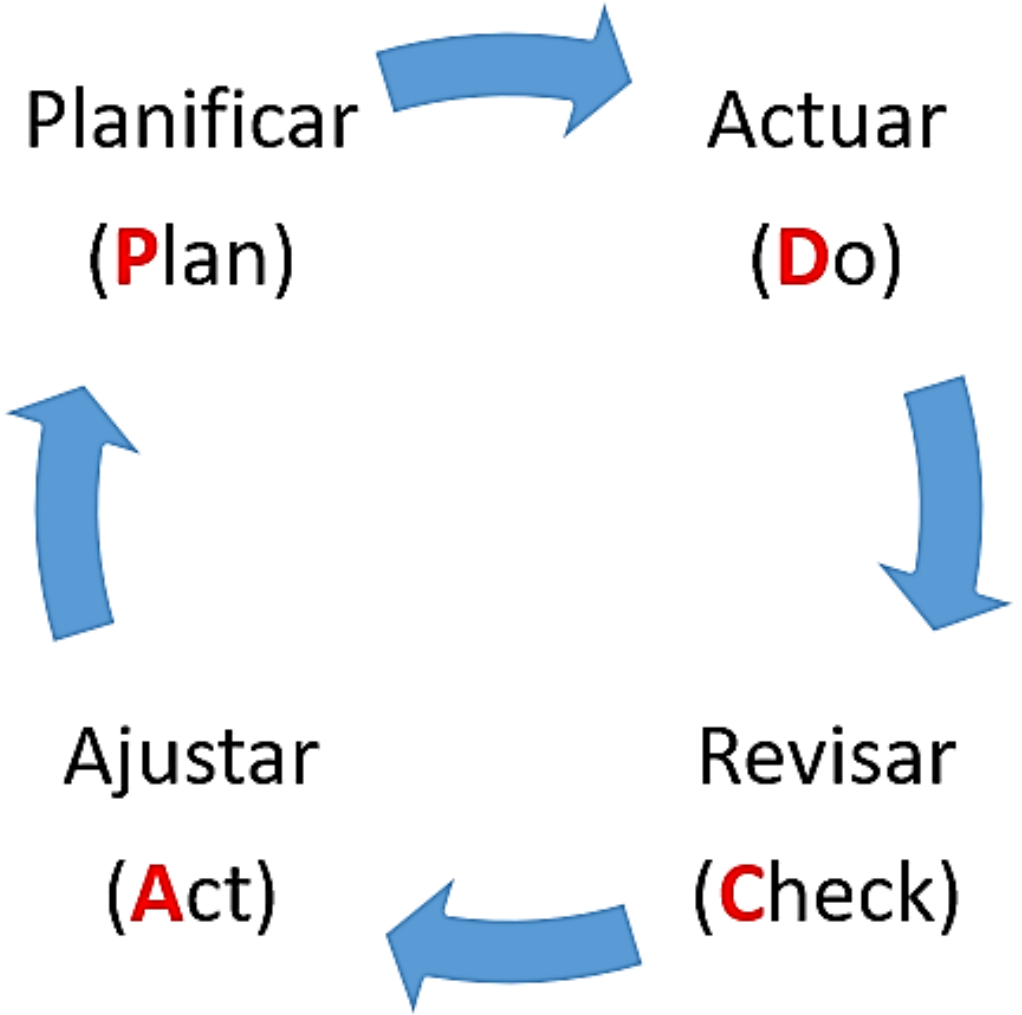
5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

SE TRATA DE **ANALIZAR LA EMPRESA**, Y **FIJAR SUS NECESIDADES DE SEGURIDAD INICIALES**, DE PONER EN PRÁCTICA LAS **MEDIDAS DE PROTECCIÓN** PARA LOGRAR ALCANZAR ESTAS NECESIDADES, DE SER CAPAZ DE **MEDIR SI SE HAN ALCANZADO** O NO, Y DE **DETECTAR LAS MEJORAS** EN LAS MEDIDAS DE PROTECCIÓN PARA ALCANZAR LAS NECESIDADES.

5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

LA ANTERIOR SECUENCIA DESCRIBE UNA REPETICIÓN CONTINUA DE FASES, CONSTITUYENDO UN:

CICLO DE MEJORA CONTINUA DE DEMING (PDCA)



5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

EN ESTE PROCESO DE EJECUCIÓN CONTINUO, NO SE DEBE PERDER DE VISTA EL **OBJETIVO:**

ASEGURAR LA CONTINUIDAD DEL NEGOCIO, MINIMIZANDO LOS RIESGOS, MAXIMIZANDO EL RETORNO DE LA INVERSIÓN Y PERMITIENDO NUEVAS OPORTUNIDADES PARA LA EMPRESA

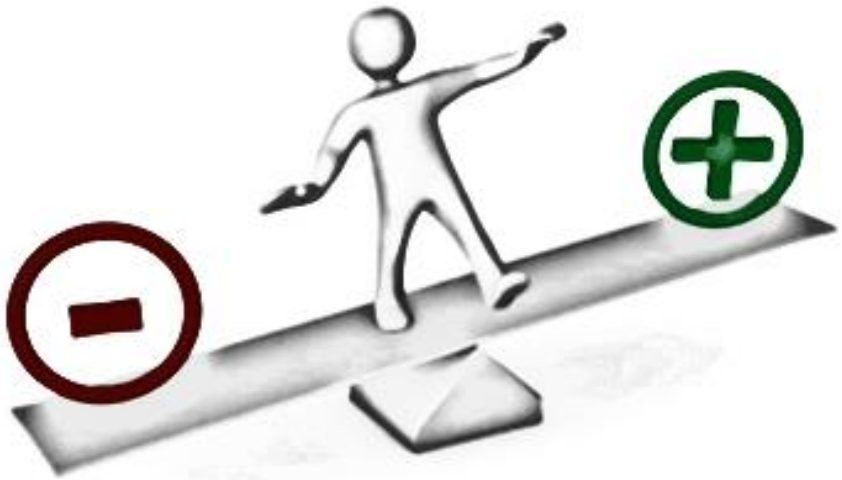
5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

UNA EMPRESA PEQUEÑA O MEDIANA (PYME) PUEDE ENFRENTAR SERIAS DIFICULTADES PARA ABORDAR LA IMPLANTACIÓN DE UN SGSI.

LA SOLUCIÓN ES SENCILLA, Y CONSISTE EN APLICAR UN PRINCIPIO MUY FRECUENTE EN EL ÁMBITO DE LA SEGURIDAD DE LA INFORMACIÓN:

EL PRINCIPIO DE PROPORCIONALIDAD

QUE NOS DICE QUE *LAS MEDIDAS DEBEN ADECUARSE A SUS OBJETIVOS*.



LAS SALVAGUARDAS DEBEN SER PROPORCIONALES AL RIESGO

5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

LAS HERRAMIENTAS ELEMENTALES PARA LA CORRECTA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SON DOS:

- **LA REDACCIÓN DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**, QUE RECOJA DE LAS DIRECTRICES DEL SGSI A PARTIR DE LAS CUALES DERIVARÁN TODAS LAS DEMÁS ACCIONES.
- **LA ADOPCIÓN DE UNA METODOLOGÍA SENCILLA**, QUE PERMITA EVALUAR EL RIESGO.

AMBAS HERRAMIENTAS PERMITEN DAR LOS PASOS DE PLANIFICACIÓN Y MEDIDA, Y SERÁN LAS ARMAS ESENCIALES DE UN SGSI

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. SENCILLAMENTE, 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; POR EJEMPLO, Y RESPECTIVAMENTE, UN INCENDIO, UNA DESCONEXIÓN ACCIDENTAL DE UN CABLE DE ALIMENTACIÓN, O UN VIRUS INFORMÁTICO


ESTO ES
TODO