IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UD01

ANEXO

CONCEPTOS DE SEGURIDAD INFORMÁTICA

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. **OBJETIVOS DE LA SEGURIDAD INFORMÁTICA**
2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN
3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

ENTRE LOS PRINCIPALES **OBJETIVOS** DE LA SEGURIDAD INFORMÁTICA PODRÍAMOS DESTACAR LOS SIGUIENTES:

- **MINIMIZAR Y GESTIONAR LOS RIESGOS** Y DETECTAR LOS POSIBLES PROBLEMAS Y AMENAZAS A LA SEGURIDAD.
- GARANTIZAR LA **ADECUADA UTILIZACIÓN DE LOS RECURSOS** Y DE LAS APLICACIONES DEL SISTEMA.
- **LIMITAR LAS PÉRDIDAS** Y CONSEGUIR LA **ADECUADA RECUPERACIÓN DEL SISTEMA** EN CASO DE UN INCIDENTE DE SEGURIDAD.
- **CUMPLIR CON EL MARCO LEGAL Y** CON **LOS REQUISITOS** IMPUESTOS POR LOS CLIENTES **EN SUS CONTRATOS**.

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

PARA CUMPLIR CON ESTOS OBJETIVOS UNA ORGANIZACIÓN DEBE CONTEMPLAR **CUATRO PLANOS DE ACTUACIÓN:**

- **TÉCNICO:** TANTO A NIVEL FÍSICO COMO A NIVEL LÓGICO.
- **LEGAL:** ALGUNOS PAÍSES OBLIGAN POR LEY A QUE EN DETERMINADOS SECTORES SE IMPLANTEN UNA SERIE DE MEDIDAS DE SEGURIDAD (SECTOR DE SERVICIOS FINANCIEROS Y SECTOR SANITARIO EN ESTADOS UNIDOS, PROTECCIÓN DE DATOS PERSONALES EN TODOS LOS ESTADOS MIEMBROS DE LA UNIÓN EUROPEA, ETCÉTERA).
- **HUMANO:** SENSIBILIZACIÓN Y FORMACIÓN DE EMPLEADOS Y DIRECTIVOS, DEFINICIÓN DE FUNCIONES Y OBLIGACIONES DEL PERSONAL...
- **ORGANIZATIVO:** DEFINICIÓN E IMPLANTACIÓN DE POLÍTICAS DE SEGURIDAD, PLANES, NORMAS, PROCEDIMIENTOS Y BUENAS PRÁCTICAS DE ACTUACIÓN.

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

Plano Humano

- Sensibilización y formación
- Funciones, obligaciones y responsabilidades del personal
- Control y supervisión de los empleados

Plano Técnico

- Selección, instalación, configuración y actualización de soluciones HW y SW
- Criptografía
- Estandarización de productos
- Desarrollo seguro de aplicaciones

Organización

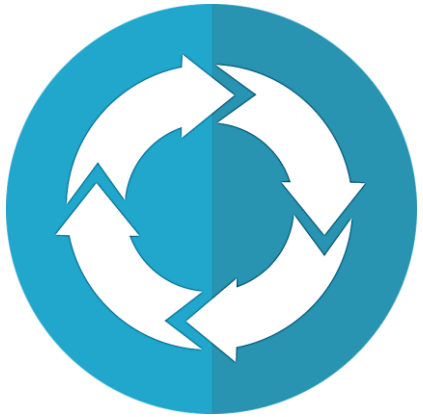
- Políticas, Normas y Procedimientos
- Planes de Contingencia y Respuesta a Incidentes
- Relaciones con terceros (clientes, proveedores...)

Legislación

- Cumplimiento y adaptación a la legislación vigente:
  - LOPD, LSSI, LGT, Firma Electrónica, Código Penal, Propiedad Intelectual...

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

UNA ORGANIZACIÓN DEBE ENTENDER **LA SEGURIDAD INFORMÁTICA COMO UN PROCESO Y NO COMO UN PRODUCTO** QUE SE PUEDA "COMPRAR" O "INSTALAR".



SE TRATA DE UN CICLO ITERATIVO, EN EL QUE SE INCLUYEN ACTIVIDADES COMO LA *VALORACIÓN DE RIESGOS, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD*.

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

LA SEGURIDAD COMO PROCESO

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

SERÍA NECESARIO CONTEMPLAR CUESTIONES COMO:

- EL **NIVEL DE CENTRALIZACIÓN/DESCENTRALIZACIÓN** DEL SISTEMA
- LA NECESIDAD DE **GARANTIZAR UN FUNCIONAMIENTO CONTINUADO** DEL SISTEMA
- EL **NIVEL DE SENSIBILIDAD** DE LOS DATOS Y DE LOS RECURSOS
- LA EXISTENCIA DE UN **ENTORNO POTENCIALMENTE HOSTIL** (CONEXIONES A REDES ABIERTAS COMO INTERNET)
- EL CUMPLIMIENTO DEL **MARCO LEGAL VIGENTE** (PROTECCIÓN DE DATOS PERSONALES, PROTECCIÓN DE LA PROPIEDAD INTELECTUAL, DELITOS INFORMÁTICOS ...)
- **CERTIFICACIÓN** BASADA EN UNA SERIE DE **ESTÁNDARES INTERNACIONALES** (**ISO 27001**)

CONTENIDOS

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA
2. **SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN**
3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

PARA PODER ALCANZAR LOS OBJETIVOS DENTRO DEL PROCESO DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA ES NECESARIO CONTEMPLAR UNA SERIE DE **SERVICIOS** O **FUNCIONES DE SEGURIDAD DE LA INFORMACIÓN**:

- **CONFIDENCIALIDAD**
- **AUTENTICACIÓN**
- **INTEGRIDAD**
- **NO REPUDIACIÓN**
- **DISPONIBILIDAD**
- **AUTORIZACIÓN**
- **AUDITABILIDAD**
- **RECLAMACIÓN DE ORIGEN**
- **RECLAMACIÓN DE PROPIEDAD**
- **ANONIMATO EN EL USO DE LOS SERVICIOS**
- **PROTECCIÓN A LA RÉPLICA**
- **CONFIRMACIÓN DE LA PRESTACIÓN DE UN SERVICIO O LA REALIZACIÓN DE UNA TRANSACCIÓN**
- **REFERENCIA TEMPORAL**
- **CERTIFICACIÓN MEDIANTE TERCEROS DE CONFIANZA**

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

CONFIDENCIALIDAD

MEDIANTE ESTE SERVICIO O FUNCIÓN DE SEGURIDAD SE **GARANTIZA QUE CADA MENSAJE TRANSMITIDO O ALMACENADO EN UN SISTEMA INFORMÁTICO SÓLO PODRÁ SER LEÍDO POR SU LEGÍTIMO DESTINATARIO.**

SI DICHO MENSAJE CAE EN MANOS DE TERCERAS PERSONAS, ÉSTAS NO PODRÁN ACCEDER AL CONTENIDO DEL MENSAJE ORIGINAL.

ESTE SERVICIO **PRETENDE GARANTIZAR LA CONFIDENCIALIDAD DE LOS DATOS ALMACENADOS** EN UN EQUIPO, DE **LOS DATOS GUARDADOS** EN DISPOSITIVOS DE BACKUP **Y/O DE LOS DATOS TRANSMITIDOS** A TRAVÉS DE REDES DE COMUNICACIONES

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

AUTENTICACIÓN

GARANTIZA QUE LA IDENTIDAD DEL CREADOR DE UN MENSAJE O DOCUMENTO ES LEGÍTIMA. GRACIAS A ESTA FUNCIÓN, EL DESTINATARIO DE UN MENSAJE PODRÁ ESTAR SEGURO DE QUE SU CREADOR ES LA PERSONA QUE FIGURA COMO REMITENTE DE DICHO MENSAJE .

TAMBIÉN PODEMOS HABLAR DE LA **AUTENTICIDAD DE UN EQUIPO** QUE SE CONECTA A UNA RED O INTENTA ACCEDER A UN DETERMINADO SERVICIO.

LA **AUTENTICACIÓN PUEDE SER UNILATERAL**, CUANDO SÓLO SE GARANTIZA LA IDENTIDAD DEL QUE SE INTENTA CONECTAR A LA RED **O MUTUA**, EN EL CASO DE QUE LA RED O EL SERVIDOR TAMBIÉN SE AUTENTICA DE CARA AL EQUIPO, USUARIO O TERMINAL QUE ESTABLECE LA CONEXIÓN.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

INTEGRIDAD

LA FUNCIÓN DE INTEGRIDAD SE ENCARGA DE **GARANTIZAR QUE UN MENSAJE O FICHERO NO HA SIDO MODIFICADO DESDE SU CREACIÓN O DURANTE SU TRANSMISIÓN A TRAVÉS DE UNA RED INFORMÁTICA.**

DE ESTE MODO , ES POSIBLE DETECTAR SI SE HA AÑADIDO O ELIMINADO ALGÚN DATO EN UN MENSAJE O FICHERO ALMACENADO, PROCESADO O TRANSMITIDO POR UN SISTEMA O RED INFORMÁTICA.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

NO REPUDIACIÓN

EL OBJETO DE ESTE SERVICIO DE SEGURIDAD **CONSISTE EN IMPLEMENTAR UN MECANISMO PROBATORIO QUE PERMITA DEMOSTRAR LA AUTORÍA Y ENVÍO DE UN DETERMINADO MENSAJE,** DE FORMA QUE EL USUARIO QUE LO HA CREADO Y ENVIADO A TRAVÉS DEL SISTEMA NO PUEDA NEGAR ESTA CIRCUNSTANCIA, SITUACIÓN QUE TAMBIÉN SE APLICA AL DESTINATARIO DEL ENVÍO.

ES UN ASPECTO DE ESPECIAL IMPORTANCIA EN LAS TRANSACCIONES COMERCIALES QUE PERMITE PROPORCIONAR A COMPRADORES Y VENDEDORES UNA SEGURIDAD JURÍDICA QUE VA A ESTAR SOPORTADA POR ESTE SERVICIO.

EN UN SISTEMA INFORMÁTICO **SE PUEDE DISTINGUIR ENTRE LA NO REPUDIACIÓN DE ORIGEN Y LA NO REPUDIACIÓN DE DESTINO**.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

DISPONIBILIDAD

SE DEBE DISEÑAR UN SISTEMA LO SUFICIENTEMENTE ROBUSTO FRENTE A ATAQUES E INTERFERENCIAS COMO PARA **GARANTIZAR SU CORRECTO FUNCIONAMIENTO, DE MANERA QUE PUEDA ESTAR PERMANENTEMENTE A DISPOSICIÓN DE LOS USUARIOS QUE DESEEN ACCEDER A SUS SERVICIOS.**

DENTRO DE LA DISPONIBILIDAD **TAMBIÉN DEBEMOS CONSIDERAR LA RECUPERACIÓN DEL SISTEMA** FRENTE A POSIBLES INCIDENTES DE SEGURIDAD, ASÍ COMO FRENTE A DESASTRES NATURALES O INTENCIONADOS.

DEBEMOS TENER EN CUENTA QUE DE NADA SIRVEN LOS DEMÁS SERVICIOS DE SEGURIDAD SI EL SISTEMA INFORMÁTICO NO SE ENCUENTRA DISPONIBLE PARA QUE PUEDA SER UTILIZADO POR SUS LEGÍTIMOS USUARIOS Y PROPIETARIOS.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

AUTORIZACIÓN (CONTROL DE ACCESO A EQUIPOS Y SERVICIOS)

MEDIANTE EL SERVICIO DE AUTORIZACIÓN SE PERSIGUE **CONTROLAR EL ACCESO DE LOS USUARIOS A LOS DISTINTOS EQUIPOS Y SERVICIOS OFRECIDOS POR EL SISTEMA INFORMÁTICO, UNA VEZ SUPERADO EL PROCESO DE AUTENTICACIÓN DE CADA USUARIO**.

PARA ELLO, SE DEFINEN UNAS **LISTAS DE CONTROL DE ACCESO (ACL)** CON LA RELACIÓN DE USUARIOS Y GRUPOS DE USUARIOS Y SUS DISTINTOS PERMISOS DE ACCESO A LOS RECURSOS DEL SISTEMA.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

AUDITABILIDAD

EL SERVICIO DE AUDITABILIDAD O TRAZABILIDAD PERMITE **REGISTRAR Y MONITORIZAR LA UTILIZACIÓN DE LOS DISTINTOS RECURSOS DEL SISTEMA POR PARTE DE LOS USUARIOS QUE HAN SIDO PREVIAMENTE AUTENTICADOS Y AUTORIZADOS .**

DE ESTE MODO, **ES POSIBLE DETECTAR SITUACIONES O COMPORTAMIENTOS ANÓMALOS** POR PARTE DE LOS USUARIOS, ADEMÁS DE **LLEVAR UN CONTROL DEL RENDIMIENTO DEL SISTEMA** (TRÁFICO CURSADO, INFORMACIÓN ALMACENADA Y VOLUMEN DE TRANSACCIONES REALIZADAS, POR CITAR ALGUNAS DE LAS MÁS IMPORTANTES).

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

RECLAMACIÓN DE ORIGEN

MEDIANTE LA RECLAMACIÓN DE ORIGEN EL SISTEMA **PERMITE PROBAR QUIÉN HA SIDO EL CREADOR DE UN DETERMINADO MENSAJE O DOCUMENTO.**

RECLAMACIÓN DE PROPIEDAD

ESTE SERVICIO PERMITE **PROBAR QUE UN DETERMINADO DOCUMENTO O UN CONTENIDO DIGITAL PROTEGIDO POR DERECHOS DE AUTOR** (CANCIÓN, VÍDEO, LIBRO...) **PERTENECE A UN DETERMINADO USUARIO** U ORGANIZACIÓN QUE OSTENTA LA TITULARIDAD DE LOS DERECHOS DE AUTOR.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

ANONIMATO EN EL USO DE LOS SERVICIOS

EN LA UTILIZACIÓN DE DETERMINADOS SERVICIOS PODRÍA RESULTAR CONVENIENTE **GARANTIZAR EL ANONIMATO DE LOS USUARIOS QUE ACCEDEN A LOS RECURSOS Y CONSUMEN DETERMINADOS TIPOS DE SERVICIOS, PRESERVANDO DE ESTE MODO SU PRIVACIDAD**.

ESTE SERVICIO DE SEGURIDAD PODRÍA ENTRAR EN CONFLICTO CON OTROS, COMO LA AUTENTICACIÓN O LA AUDITORÍA DEL ACCESO A LOS RECURSOS.

LA CRECIENTE PREOCUPACIÓN DE LOS GOBIERNOS POR EL CONTROL E INTERCEPTACIÓN DE TODO TIPO DE COMUNICACIONES ANTE EL PROBLEMA DEL TERRORISMO INTERNACIONAL ESTÁ PROVOCANDO LA ADOPCIÓN DE NUEVAS MEDIDAS PARA RESTRINGIR EL ANONIMATO Y LA PRIVACIDAD DE LOS CIUDADANOS QUE UTILIZAN ESTOS SERVICIOS.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

PROTECCIÓN A LA RÉPLICA

MEDIANTE ESTE SERVICIO DE SEGURIDAD SE TRATA DE **IMPEDIR LA REALIZACIÓN DE ATAQUES DE REPETICIÓN POR PARTE DE USUARIOS MALICIOSOS, CONSISTENTES EN LA INTERCEPTACIÓN Y POSTERIOR REENVÍO DE MENSAJES PARA TRATAR DE ENGAÑAR AL SISTEMA Y PROVOCAR OPERACIONES NO DESEADAS**, COMO PODRÍA SER EL CASO DE REALIZAR VARIAS VECES UNA MISMA TRANSACCIÓN BANCARIA

EN ESTE SERVICIO SE SUELE RECURRIR A LA UTILIZACIÓN DE UN NÚMERO DE SECUENCIA O SELLO TEMPORAL EN TODOS LOS MENSAJES Y DOCUMENTOS QUE NECESITEN SER PROTEGIDOS DENTRO DEL SISTEMA, DE FORMA QUE SE PUEDAN DETECTAR Y ELIMINAR POSIBLES REPETICIONES DE MENSAJES QUE YA HAYAN SIDO RECIBIDOS POR EL DESTINATARIO.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

CONFIRMACIÓN (PRESTACIÓN DE UN SERVICIO O REALIZACIÓN DE TRANSACCIÓN)

ESTE SERVICIO DE SEGURIDAD **PERMITE CONFIRMAR LA REALIZACIÓN DE UNA OPERACIÓN O TRANSACCIÓN**, REFLEJANDO LOS USUARIOS O ENTIDADES QUE HAN INTERVENIDO EN ÉSTA.

REFERENCIA TEMPORAL (CERTIFICACIÓN DE FECHAS)

MEDIANTE ESTE SERVICIO DE SEGURIDAD SE CONSIGUE **DEMOSTRAR EL INSTANTE CONCRETO EN QUE SE HA ENVIADO UN MENSAJE O SE HA REALIZADO UNA DETERMINADA OPERACIÓN.**

SE SUELE RECURRIR AL **SELLADO TEMPORAL** DEL MENSAJE O DOCUMENTO EN CUESTIÓN.

2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

CERTIFICACIÓN MEDIANTE TERCEROS DE CONFIANZA

LA REALIZACIÓN DE TODO TIPO DE **TRANSACCIONES** A TRAVÉS DE MEDIOS ELECTRÓNICOS **REQUIERE** DE NUEVOS REQUISITOS DE SEGURIDAD, PARA **GARANTIZAR LA AUTENTICACIÓN DE LAS PARTES** QUE INTERVIENEN, **EL CONTENIDO E INTEGRIDAD DE LOS MENSAJES O LA CONSTATACIÓN DE LA REALIZACIÓN DE LA OPERACIÓN** EN UN DETERMINADO INSTANTE TEMPORAL.

PARA ESTO, SE RECURRE A LA FIGURA DEL **TERCERO DE CONFIANZA**, ORGANISMO QUE **SE ENCARGA DE CERTIFICAR** LA REALIZACIÓN Y EL CONTENIDO DE **LAS OPERACIONES Y DE AVALAR LA IDENTIDAD DE LOS INTERVINIENTES**, DOTANDO DE ESTE MODO A LAS TRANSACCIONES ELECTRÓNICAS DE UNA MAYOR SEGURIDAD JURÍDICA.

CONTENIDOS

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA
2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN
3. **CONSECUENCIAS DE LA FALTA DE SEGURIDAD**

3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

ACTUALMENTE LAS ACTIVIDADES DE **MUCHAS ORGANIZACIONES DEPENDEN DE LOS DATOS E INFORMACIÓN REGISTRADOS EN SUS SISTEMAS INFORMÁTICOS**, ASÍ COMO DEL SOPORTE ADECUADO PARA FACILITAR SU ALMACENAMIENTO, PROCESAMIENTO, ANÁLISIS Y DISTRIBUCIÓN.

LA ELIMINACIÓN DE TODAS LAS TRANSACCIONES DE UN DÍA EN UNA EMPRESA PODRÍA OCASIONARLE MÁS PÉRDIDAS ECONÓMICAS QUE SUFRIR UN ROBO O UN ACTO DE SABOTAJE CONTRA ALGUNA DE SUS INSTALACIONES.

3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

EN CONSECUENCIA, **ES IMPORTANTE PONER EN CONOCIMIENTO** DE LOS DIRECTIVOS CUÁL ES **EL COSTE E IMPACTO DE LOS INCIDENTES DE SEGURIDAD EN TÉRMINOS ECONÓMICOS**.

LA INVERSIÓN EN SEGURIDAD INFORMÁTICA SERÍA COMPARABLE A LA CONTRATACIÓN DE UN SEGURO CONTRA ROBOS, CONTRA INCENDIOS O DE RESPONSABILIDAD CIVIL FRENTE A TERCEROS.

3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

LA IMPLANTACIÓN DE DETERMINADAS MEDIDAS DE SEGURIDAD PUEDE REPRESENTAR UN **IMPORTANTE ESFUERZO ECONÓMICO** PARA UNA ORGANIZACIÓN.

ES NECESARIO **REALIZAR UN ANÁLISIS PRELIMINAR** DE LAS POSIBLES PÉRDIDAS PARA LA ORGANIZACIÓN Y UNA EVALUACIÓN DE LOS RIESGOS:

¿QUÉ PUEDE IR MAL?

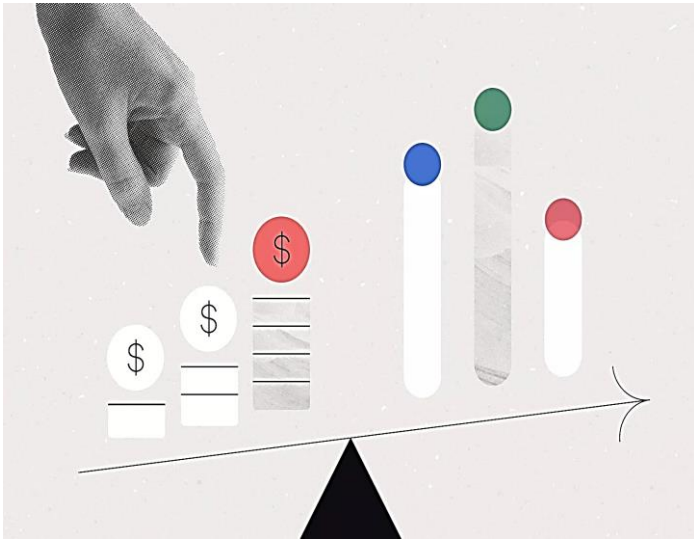
¿CON QUÉ FRECUENCIA PUEDE OCURRIR?

¿CUÁLES SERÍAN SUS CONSECUENCIAS PARA LA ORGANIZACIÓN?...

3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

EL OBJETIVO PERSEGUIDO ES **LOGRAR QUE UN ATAQUE** CONTRA LOS RECURSOS O LA INFORMACIÓN PROTEGIDA **TENGA UN COSTE SUPERIOR PARA EL ATACANTE QUE EL VALOR EN EL MERCADO DE ESTOS BIENES**.

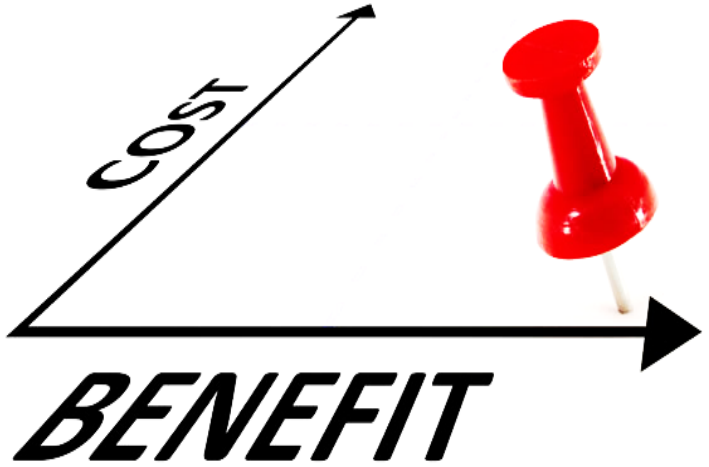
ADEMÁS, SIEMPRE **SE DEBE TENER EN CUENTA QUE EL COSTE DE LAS MEDIDAS ADOPTADAS POR LA ORGANIZACIÓN HA DE SER MENOR QUE EL VALOR DE LOS ACTIVOS A PROTEGER**.



3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

PARA ELLO, ES NECESARIO REALIZAR UN ANÁLISIS DE LA **RELACIÓN COSTE/BENEFICIO DE CADA MEDIDA DE SEGURIDAD** QUE SE DESEE IMPLANTAR, YA QUE **NO TODAS LAS ORGANIZACIONES PRECISAN DE LAS MISMAS MEDIDAS DE SEGURIDAD**.

DE HECHO, CADA ORGANIZACIÓN PUEDE TENER DISTINTAS EXPECTATIVAS DE SEGURIDAD.



3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

ADEMÁS DE LOS POSIBLES **DAÑOS** OCASIONADOS A LA INFORMACIÓN GUARDADA Y A LOS EQUIPOS Y DISPOSITIVOS DE RED, **DEBERÍAMOS TENER EN CUENTA OTROS IMPORTANTES PERJUICIOS PARA LA ORGANIZACIÓN**:

- **HORAS DE TRABAJO INVERTIDAS** EN LAS REPARACIONES Y RECONFIGURACIÓN DE LOS EQUIPOS Y REDES.
- **PÉRDIDAS OCASIONADAS POR LA INDISPONIBILIDAD DE DIVERSAS APLICACIONES Y SERVICIOS INFORMÁTICOS**: COSTE DE OPORTUNIDAD POR NO PODER UTILIZAR ESTOS RECURSOS.
- **ROBO DE INFORMACIÓN CONFIDENCIAL Y SU POSIBLE REVELACIÓN A TERCEROS NO AUTORIZADOS:** FÓRMULAS, DISEÑOS DE PRODUCTOS, ESTRATEGIAS COMERCIALES, PROGRAMAS INFORMÁTICOS...

3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

- **FILTRACIÓN DE DATOS PERSONALES DE USUARIOS REGISTRADOS EN EL SISTEMA:** EMPLEADOS, CLIENTES, PROVEEDORES, CONTACTOS COMERCIALES O CANDIDATOS DE EMPLEO, CON LAS CONSECUENCIAS QUE SE DERIVAN DEL INCUMPLIMIENTO DE LA LEGISLACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES VIGENTES EN TODA LA UNIÓN EUROPEA Y EN MUCHOS OTROS PAÍSES.
- **POSIBLE IMPACTO EN LA IMAGEN DE LA EMPRESA ANTE TERCEROS:** PÉRDIDA DE CREDIBILIDAD EN LOS MERCADOS, DAÑO A LA REPUTACIÓN DE LA EMPRESA, PÉRDIDA DE CONFIANZA POR PARTE DE LOS CLIENTES Y LOS PROVEEDORES, ETC.

3. CONSECUENCIAS DE LA FALTA DE SEGURIDAD

- **RETRASOS EN LOS PROCESOS DE PRODUCCIÓN,** PÉRDIDA DE PEDIDOS, IMPACTO EN LA CALIDAD DEL SERVICIO, PÉRDIDA DE OPORTUNIDADES DE NEGOCIO...
- POSIBLES **DAÑOS A LA SALUD DE LAS PERSONAS**, CON PÉRDIDAS DE VIDAS HUMANAS EN LOS CASOS MÁS GRAVES.
- **PAGO DE INDEMNIZACIONES POR DAÑOS Y PERJUICIOS** A TERCEROS, TENIENDO QUE AFRONTAR ADEMÁS POSIBLES RESPONSABILIDADES LEGALES Y LA IMPOSICIÓN DE SANCIONES ADMINISTRATIVAS.


ESTO ES
TODO