EAE Business School

Inteligencia de Negocios

Business Intelligence

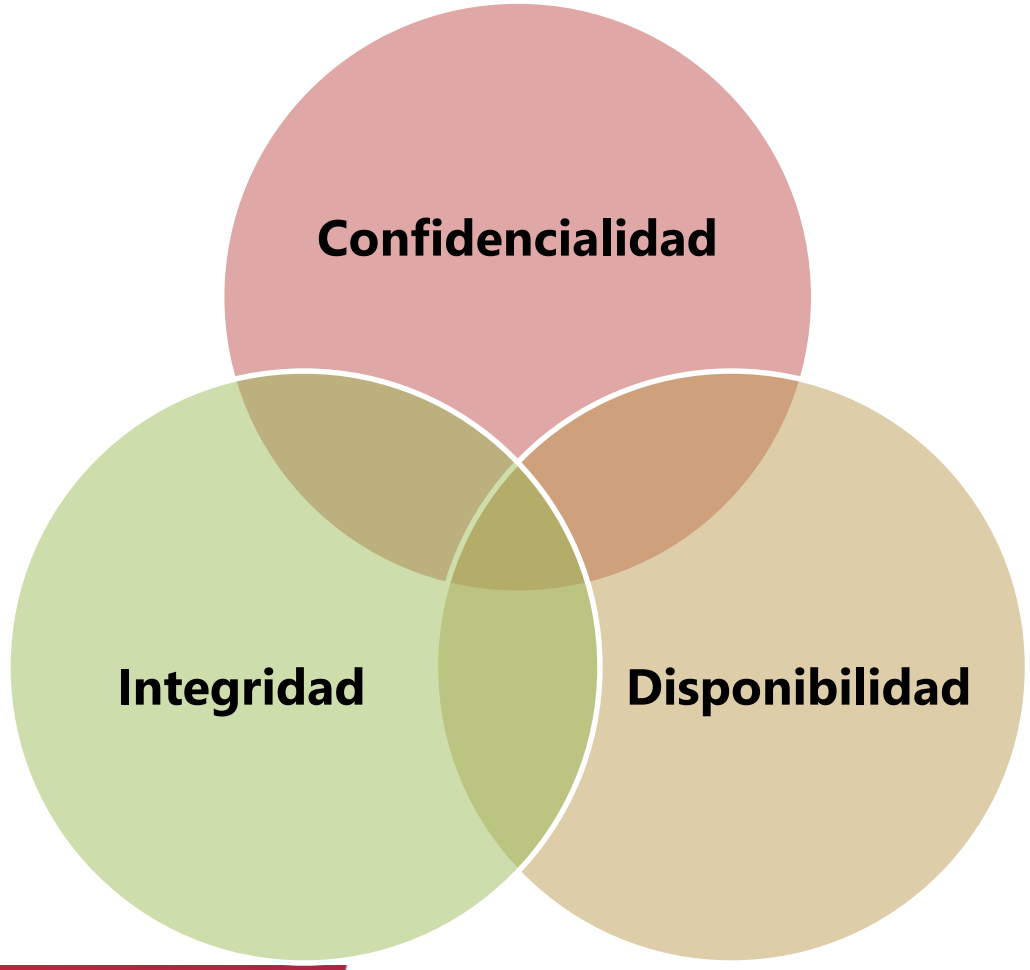
Seguridad de la Información y Seguridad Informática

Prof. Rita de la Torre

La seguridad de la información
es el conjunto de medidas
preventivas y reactivas de las
organizaciones y de los sistemas
tecnológicos que permiten
resguardar y proteger la
información buscando mantener
la confidencialidad,
la disponibilidad y
la integridad
de la misma.

La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.

La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros

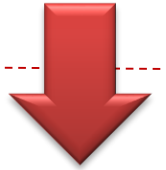


La información debe estar siempre accesible para aquellos que estén autorizados

La seguridad informática
es el área de la
informática
que se enfoca en la
protección de la
infraestructura
computacional y la
información contenida
o circulante.

DIRECCIÓN ESTRATÉGICA

SEGURIDAD DE LA INFORMACIÓN (INFORMATION SECURITY)		
ANÁLISIS DE RIESGOS (RISK ANALYSIS)	NORMATIVAS (NORMATIVE)	PLAN DIRECTOR (PROCEDURES)



TÁCTICO OPERACIONAL

SEGURIDAD INFORMÁTICA (I.T. SECURITY)		
CONFIGURACIÓN SEGURA (HARDENING))	TÉCNICAS DE PROTECCIÓN (FIREWALL, ANTIVIRUS, IDS)	EVENTOS, AUDITORÍAS (INCIDENT MANAGEMENT)

CUMPLIMIENTO NORMATIVO

- Exigencias legales
- Normas sectoriales
- Estándares
- Medidas dispuestas por clientes

SEGURIDAD INFORMÁTICA

- Sistemas antimalware
- Protección anti-hackers
- Copias de seguridad
- Criptografía

PROCESOS DE SEGURIDAD

- Identificación y valoración de activos
- Análisis de riesgos
- Roles y responsabilidades
- Medidas aplicadas y sus resultados

VIGILANCIA DE SEGURIDAD

- Aplica tanto a I.T. como a procesos.
- Reduce la incertidumbre.
- Existen IRPs
- Control gráfico
- Informes y Cuadros de Mando

Gestión de Riesgos

Prof. Rita de la Torre

En términos de gestión de riesgos de seguridad de la información, el activo principal a proteger es la información de la compañía.

Además de la información se debe considerar: infraestructura informática, equipos auxiliares, redes de comunicaciones, instalaciones y personas.

Aparte de medir las posibles consecuencias se ha de estimar la probabilidad de que ocurran los incidentes.

La norma **ISO 27001:2013** incluye una lista de controles de aplicación a la mayoría de empresas.

https://www.youtube.com/watch?v=ETC6NlcNlC4

Primarios

- ✓ **información**: estratégica, de carácter personal o que esté sujeta a legislación que la proteja, esencial para el desarrollo del negocio, de difícil o muy costosa reposición, etc
- ✓ **actividades y procesos de negocio**: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc

De soporte

- ✓ **hardware**: PC, portátiles, servidores, impresoras, discos
- ✓ **software**: sistemas operativos, paquetes, aplicaciones, ...
- ✓ **documentos en papel**
- ✓ **redes**: conmutadores, cableado, puntos de acceso, ...
- ✓ **personal**: usuarios, desarrolladores, responsables, ...
- ✓ **edificios**: salas, y sus servicios
- ✓ **estructura organizativa**: responsables, áreas, contratistas

Las amenazas a las que se enfrenta la información pueden ser muy variadas:

- de origen natural: inundaciones, terremotos, incendios, rayos
- fallos de la infraestructura auxiliar: fallos de suministro eléctrico, refrigeración, contaminación…
- fallos de los sistemas informáticos y de comunicaciones: fallos en las aplicaciones, hardware o equipos de transmisiones
- error humano: errores accidentales o deliberados de las personas que interactúan con la información, por ejemplo:
  - ✓ acciones no autorizadas como uso de software o hardware no autorizados
  - ✓ funcionamiento incorrecto por abuso o robo de derechos de acceso o errores en el uso, falta de disponibilidad, etc
  - ✓ información comprometida por robo de equipos, desvelado de secretos, espionaje, etc

Las vulnerabilidades frente a las cuales se debe proteger a los sistemas de información y a la información que tratan, dependen en gran medida de la naturaleza de los mismos

- Equipamiento informático susceptible a variaciones de temperatura o humedad.
- Sistemas operativos que por su estructura, configuración o mantenimiento son más vulnerables a algunos ataques.
- Localizaciones que son más propensas a desastres naturales como por ejemplo inundaciones o que están en lugares con variaciones de suministro eléctrico.
- Aplicaciones informáticas, que por su diseño, son más inseguras que otras.
- Personal sin la formación adecuada, ausente o sin supervisión

¿Cómo se mide el nivel de riesgo?

El nivel de riesgo es una estimación de lo que puede ocurrir y se valora, de forma cuantitativa, como el producto del impacto, (consecuencia), asociado a una amenaza (suceso), por la probabilidad de la misma.

Impacto x Probabilidad = Riesgo

El impacto se valora en términos del coste derivado del valor de los activos y abarca lo siguiente:

- daños personales
- pérdidas financieras
- interrupción del servicio
- pérdida de imagen y reputación
- disminución del rendimiento

1. ETAPA

IDENTIFICACIÓN DE LOS ACTIVOS SUSCEPTIBLES DE SUFRIR UNA AMENAZA

2. ETAPA

VALORACIÓN DE LOS ACTIVOS CRÍTICOS DE LA ORGANIZACIÓN

3. ETAPA

PRINCIPALES AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS

4. ETAPA

CONSECUEN-CIAS QUE PUEDE SUFRIR UN ACTIVO Y PROBABILIDAD DE QUE ESO OCURRA

5. ETAPA

MEDIDAS DE SEGURIDAD EXISTENTES QUE REDUCEN LA PROBABILIDAD O EL IMPACTO DE LAS AMENAZAS.

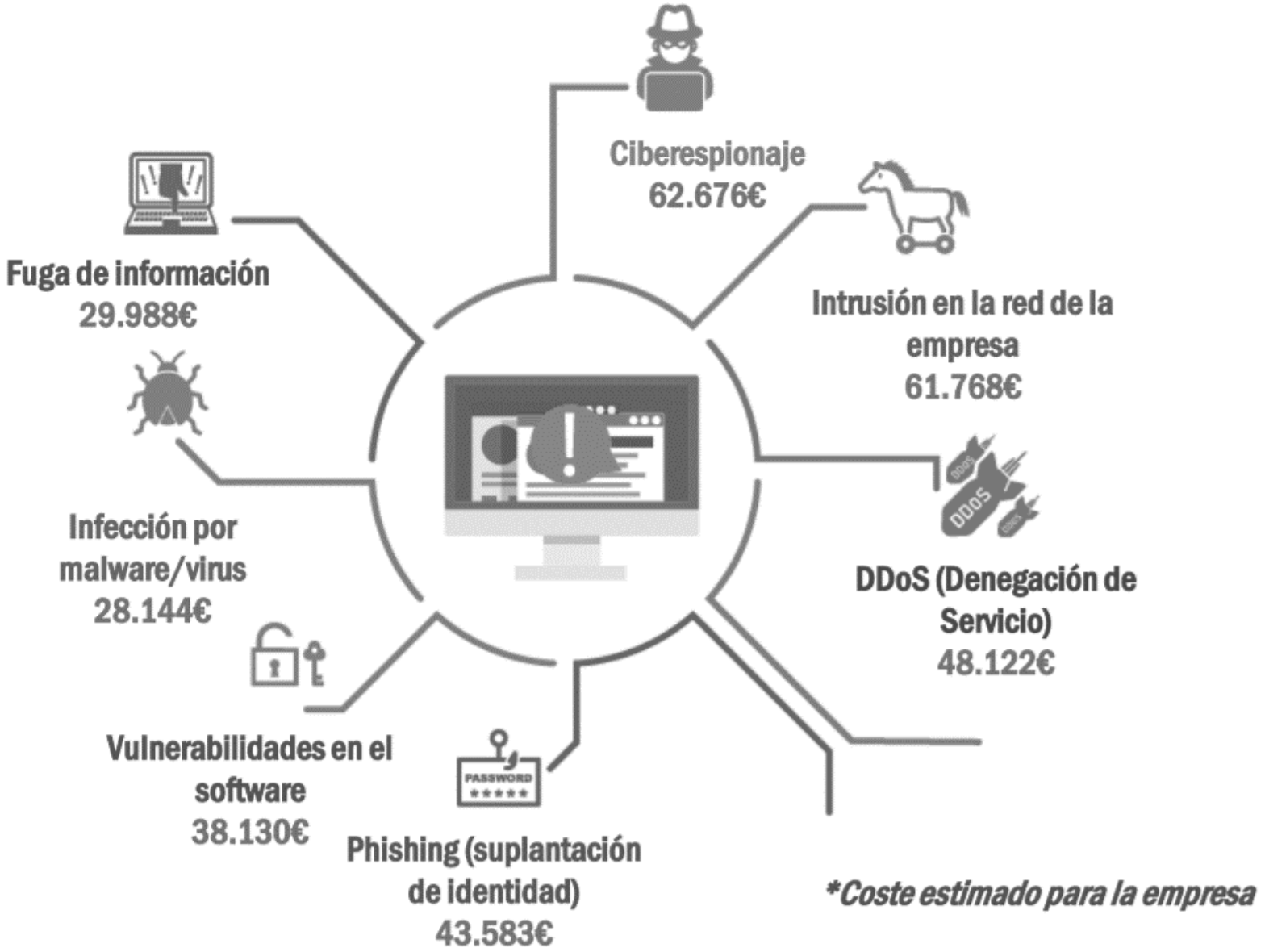
6. ETAPA

RIESGOS RESIDUALES A LOS QUE LA ORGANIZA-CIÓN ESTÁ EXPUESTA

Fuente: Dossier Plan Director de Seguridad. INCIBE

Coste promedio de incidentes de Seguridad en la PYMES

Fuente: INCIBE,
basado en el informe KASPERKY LABS



https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Soluciones de Ciberseguridad

Prof. Rita de la Torre

- gestión de acceso e identidad
- protección en el puesto de trabajo;
- seguridad en aplicaciones y datos
- seguridad en los sistemas
- seguridad en las redes

- Personas
- Información
- Infraestructura
- Negocio

El primer elemento de seguridad que es necesario proteger es el acceso a los sistemas y las aplicaciones, así como los elementos de autenticación.

Estos mecanismos son los responsables de establecer los permisos y vigilar los accesos a los sistemas y aplicaciones locales o remotas, de asignar, mantener y controlar los perfiles de los usuarios.

Estándar ISO 17799.
Control de Acceso

Son los productos que aportan seguridad en el entorno local, en el hardware y software del usuario. (ANTIVIRUS Y ANTISPAM)

Suelen incluir funciones que vigilan la actualización del software instalado en nuestros sistemas, advirtiendo de posibles amenazas

KASPERSKY ANTI-VIRUS
PANDA SECURITY
AVG
Norton by Symantec
McAfee
VIPRE ANTI VIRUS
NOD32 antivirus system

Este nivel es el encargado de dotar de seguridad a las aplicaciones y datos, desde los sistemas de almacenamiento local hasta los remotos.

Productos que cifran la información, así como los que establecen políticas de respaldo de la información, copias de seguridad (*backup*), etc.

Particular interés tienen en este alcance la protección de datos personales y la autenticación (comercio electrónico, banca online...) que en la actualidad está siendo objeto de un incremento de ataques.

https://www.servotic.com/sistemas-backup/

Las soluciones que aplican sirven con frecuencia para aplicar métodos de supervisión y mecanismos de auditoría.

Se incluyen herramientas
para servidores corporativos,
herramientas de restauración
en caso de incidentes de seguridad
para sistemas de almacenamiento,
así como herramientas de auditorías
técnicas de sistemas y gestión
de eventos de seguridad.

En este alcance se incluyen principalmente los cortafuegos (firewalls), las redes privadas virtuales (VPN), sistemas de prevención y detección de intrusiones, herramientas para la protección de redes inalámbricas y dispositivos móviles, así como herramientas para el control de tráfico de red y comunicaciones.

Aquí se garantiza la seguridad en los accesos remotos de equipos entre redes, y la transferencia de información, permitiendo solo a usuarios autorizados, la supervisión, análisis y control de los tráficos entrantes y salientes y garantizando la continuidad de conectividad de los equipos transmisores.

Los servicios bajo este alcance están relacionados con la concienciación y la formación sobre medidas de seguridad.

Los servicios de aplicación de medidas de seguridad organizativas; permisos y obligaciones, la identificación y prevención ante ataques de ingeniería social, cumplimiento con la legislación.

También están los servicios de mantenimiento de la actividad en caso de ataque, restauración de la actividad y búsqueda de los motivos del fallo de seguridad.

Se estima que el 82% de la pérdida de datos sensibles de una empresa son causados por los propios empleados

Los servicios bajo este ámbito van a permitir el intercambio de información confidencial.

También los servicios orientados a la protección frente a pérdidas de información, copias de seguridad y su posterior recuperación, los que evitan la difusión no permitida de la información y los que aplican medidas de protección.

Bajo este alcance se encuentran los servicios dirigidos a la selección, implementación y operación de las soluciones de seguridad.

Se encuentran los servicios que detectan los posibles fallos de seguridad de la infraestructura, y los que proporcionan los recursos necesarios de seguridad y la gestión de los incidentes de seguridad.

Bajo este alcance están los servicios
que facilitan los cambios organizativos
necesarios para la adecuación de los planes y políticas de seguridad dentro de las organizaciones, las normativas y los requisitos legales aplicables

https://www.incibe.es/protege-tu-empresa/kit-concienciacion

EAE Business School

We make
it happen