Seguridad 365

Elaboración SGSI Seguridad365 (Concienciación Seguridad)

Programa:	MISTIC
Empresa:	Seguridad365
Prueba:	TFM (Memoria)
Fecha:	21 de diciembre de 2018
Alumno:	José Alberto Catalá Hernansáiz
Universidad:	Universidad Oberta de Cataluña
Consultor:	Antonio José Segovia Henares

UOC Universitat Oberta de Catalunya

UAB Universitat Autònoma de Barcelona

UNIVERSITAT ROVIRA i VIRGILI

UIB Universitat de les Illes Balears

Qué es la información?

La información es un **activo** esencial para el servicio y funcionamiento de Seguridad365, y en consecuencia, necesita ser protegido adecuadamente.

La información puede estar impresa o escrita en papel, almacenada o transmitida por un sistema de información o dispositivo extraíble, presentada en imágenes, o expuesta en una conversación, pero siempre debe ser protegida de forma adecuada.

Qué es la seguridad de la información

La seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información buscando mantener las dimensiones de la misma. Se basa en la **confidencialidad**, **integridad**, **disponibilidad, autenticidad y trazabilidad**. Adicionalmente pueden estar incluidas otras propiedades, tales como: Autenticidad y Trazabilidad. El concepto de *seguridad de la información* no debe ser confundido con el de *seguridad informática*.

La seguridad de la información es un proceso continuo que actúa de forma transversal en toda la organización, y se asocia a la gestión.

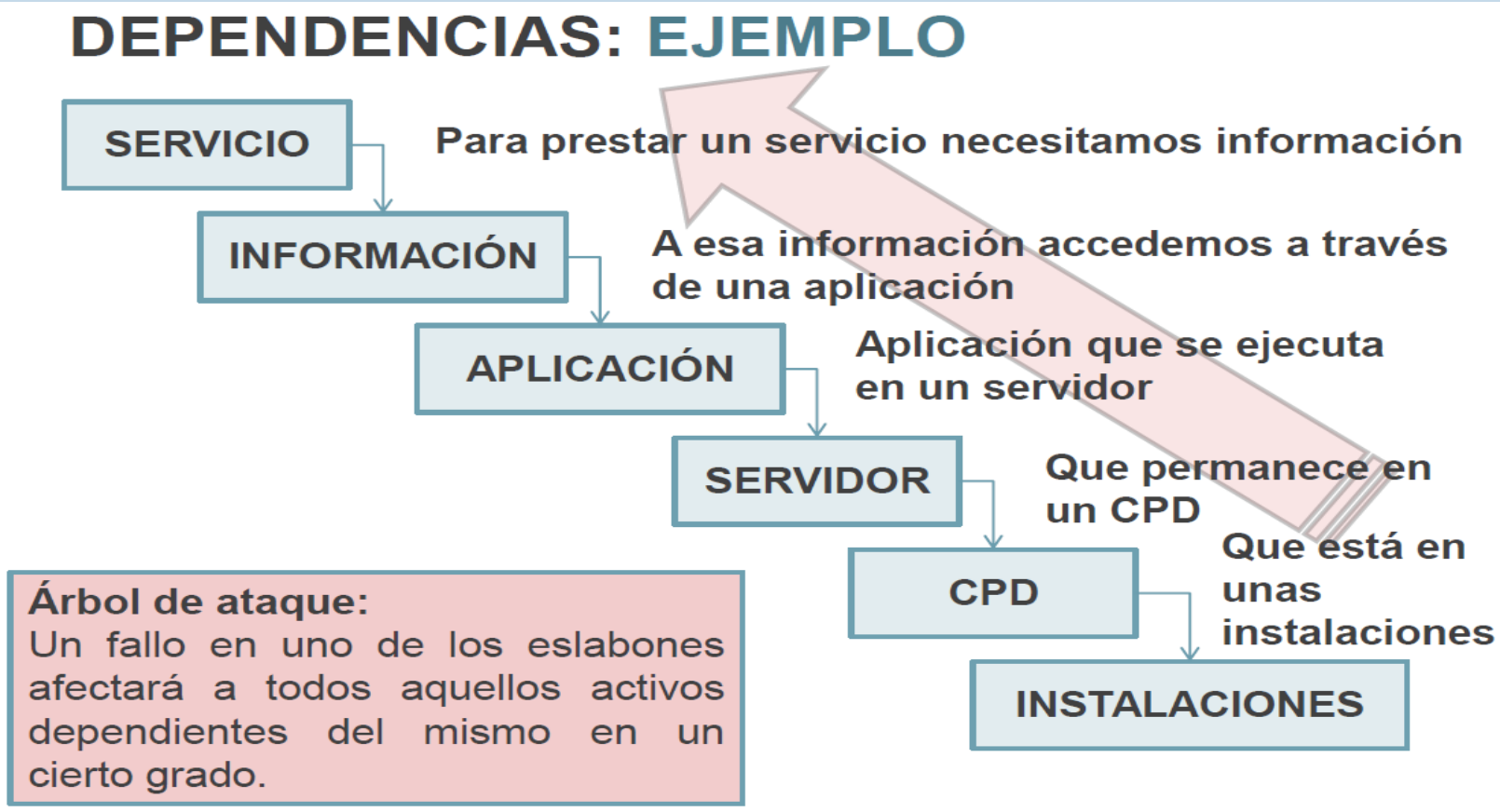
Por ello, se puede considerar la seguridad de la información en el ámbito informático como un apartado dentro de la gestión de la seguridad de la información.

Qué es la seguridad de la informació

Seguridad 365

La gestión de la seguridad de la información requiere la participación de:

TODOS los empleados



Que se protege

- ✓ Procesos / Servicios
- ✓ Información / Datos
- ✓ Aplicaciones (SW)
- ✓ Equipamiento Informático (HW)
- ✓ Redes de Comunicaciones.
- ✓ CPD
- ✓ Personal / RRHH

La Norma ISO 27001

A. ISO 27001 es la única **norma internacional auditable** que define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), concepto clave sobre el que se construye ISO 27001.

B. La información tiene una importancia fundamental para el funcionamiento y la continuidad de la organización. La implantación de ISO 27001 ayuda a gestionar y proteger los **activos de información.**

C.Exige una **implicación corporativa** en su implantación, mantenimiento y evolución.

D.Permite a los prestadores de servicios **evidenciar ante sus clientes unos niveles de protección de la información conforme a las mejores prácticas internacionales**. En organizaciones que desarrollan funciones, misiones, cometidos o servicios para las Administraciones Públicas puede implantarse de forma integrada con el Esquema Nacional de Seguridad.

La Norma ISO 27001

La norma se basa en 14 Dominios de Seguridad, 35 objetivos de control y 114 controles.

ANEXO A

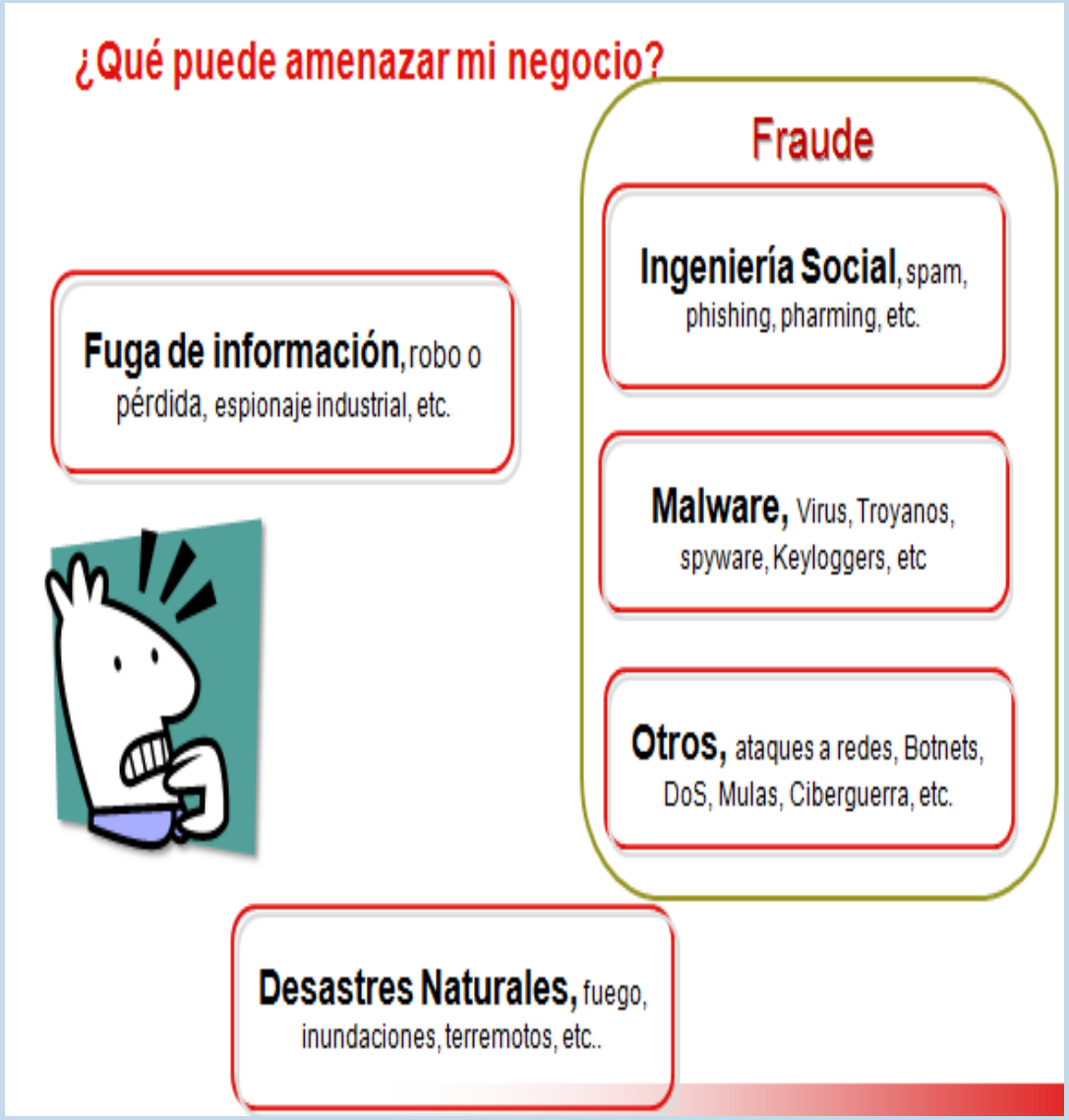
- A.5 Políticas de seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad de los recursos humanos
- A.8 Gestión de activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y ambiental
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.15 Relaciones con proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de seguridad de la información de la gestión de continuidad del negocio
- A.18 Cumplimiento

Ataques a la seguridad de la información

Qué es una Amenaza? Se define amenaza como *la intención de causar un daño a un activo de información*.

Los tipos de amenaza pueden ser múltiples: robos de medios o información, ataques externos, fallos técnicos, interrupciones de servicio, acciones no autorizadas, ataques internos, desastres naturales, etc…

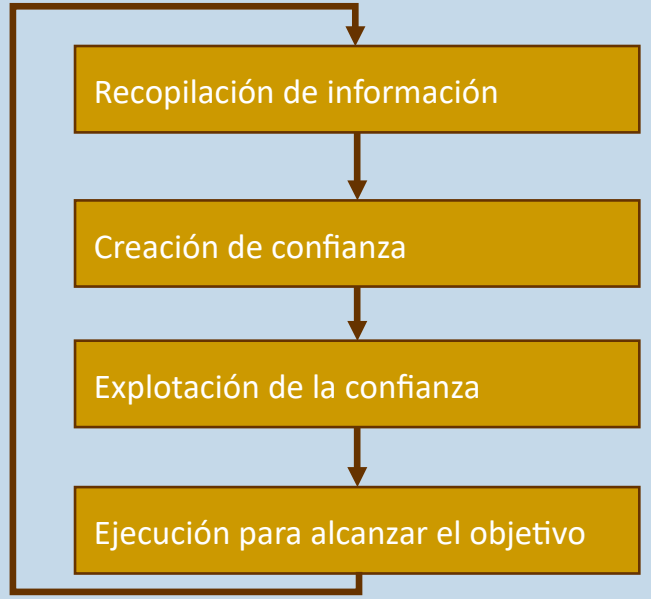
La seguridad va orientada a minimizar la probabilidad y/o el impacto de que se materialicen las amenazas.



Ingeniería social, ataques a las personas

Métodos usados por el atacante

- Simular ser personas de autoridad.
- Fingir necesitar ayuda.
- Robar la identidad.
- Pretender ser de mantenimiento/soporte.
- Software malicioso.
- Investigar a la víctima.



Las personas son siempre el eslabón

más débil en cuanto a seguridad

Ingeniería social, ataques a las personas

Existen muchas formas de sustraer información, la más usual mediante técnicas de ingeniería social, debemos desconfiar de cualquier persona no confiable. Por ejemplo, el clásico engaño de ingeniería social consistente en llamar a un empleado por teléfono haciéndose pasar como un técnico de sistemas o un nuevo compañero de otro departamento, solicitando el usuario y la contraseña para solucionar un problema urgente.

BUENAS PRÁCTICAS

Puesto de Trabajo

Protege tu ordenador y la información que contiene. Asegúrate de proteger tu equipo cuando abandonas tu entorno de trabajo. Activa el protector de pantalla; presionando la tecla "Windows" y la tecla "L" (si eres usuario de Microsoft) bloqueas el entorno y es necesaria la contraseña personal para volver a acceder.

Puesto de Trabajo

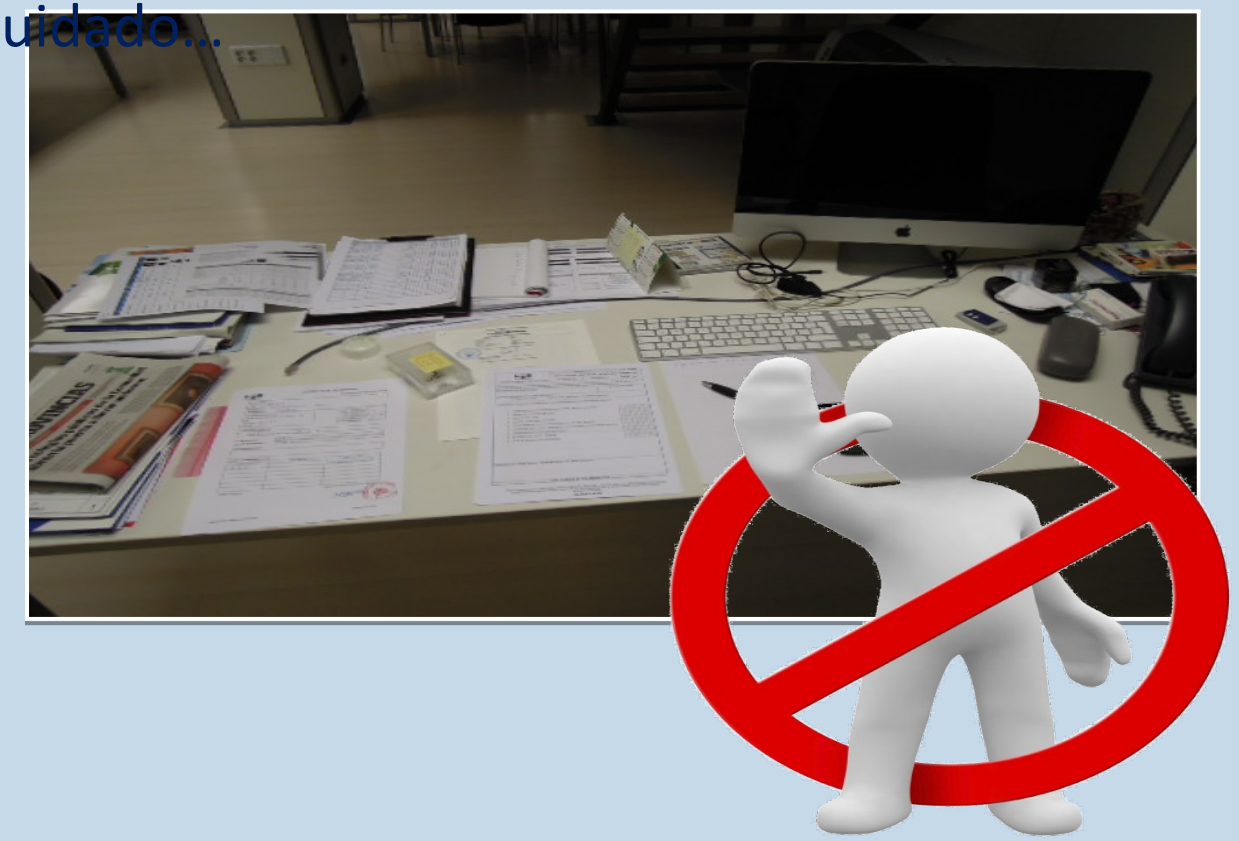
Uso adecuado de los activos de la empresa. Utiliza los soportes y equipo que te facilita la empresa de forma responsable. No alteres la configuración física o lógica de los equipos, ni instales software no autorizado, ni utilices soportes portátiles en equipos no confiables o poco seguros.

Prohibido:

- Instalar software ajeno a la empresa.
- Sacar información de la empresa sin autorización.
- Enviar e-mails masivos, con fines no profesionales.
- Intentar distorsionar o falsear registros de sistema.
- Intentar aumentar los privilegios en el sistema.
- Introducir voluntariamente malware (virus, troyanos…)

Puesto de Trabajo

No dejes papeles en tu escritorio con información confidencial. No sabes quién puede entrar y ver/llevarse los papeles que tienes encima de tu escritorio cuando no estás. Por lo tanto, debes tener mucho cuidado…



Contraseñas

Protege el acceso a tu espacio de trabajo y a tu equipo. Protege tus contraseñas corporativas y tus tarjetas de identificación como podrías guardar tu numero PIN de tu tarjeta de crédito o de tu teléfono móvil.

Evitar:

- Datos personales
- Nombre usuario
- No sea de diccionario
- No mezclar ámbito personal - profesional
- Qwerty, 111111, abcdef…

Custodia de las contraseñas:

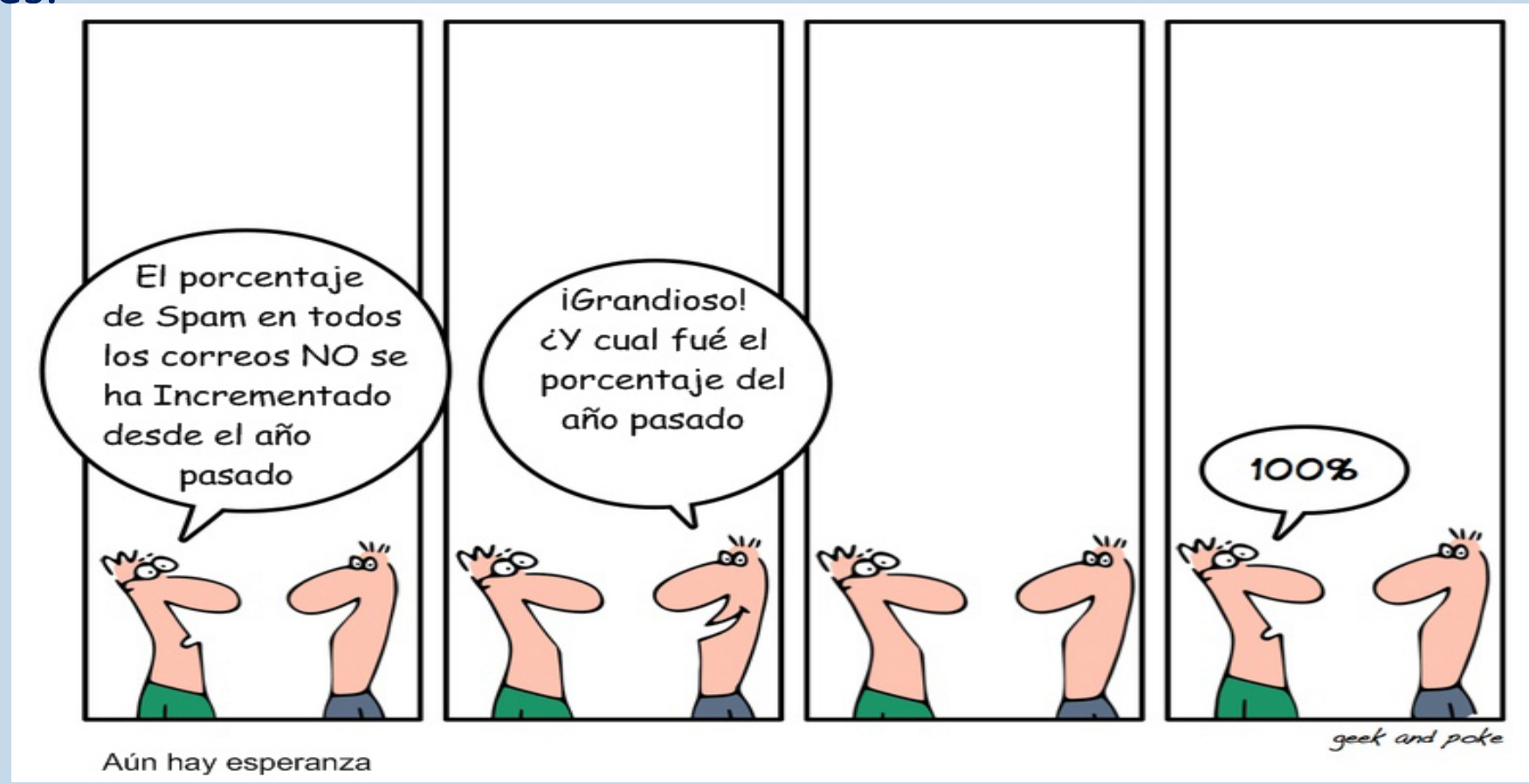
- Nunca visibles (post-it, escritas en el cuaderno… papel junto al monitor…)
- No almacenar en un fichero dentro del ordenador (sobre todo si es portátil)
- Ante sospecha, la contraseña se modificará inmediatamente.

Contraseñas

Confidencialidad de las contraseñas. No compartas ni comuniques nunca a nadie tus contraseñas.

Correo@

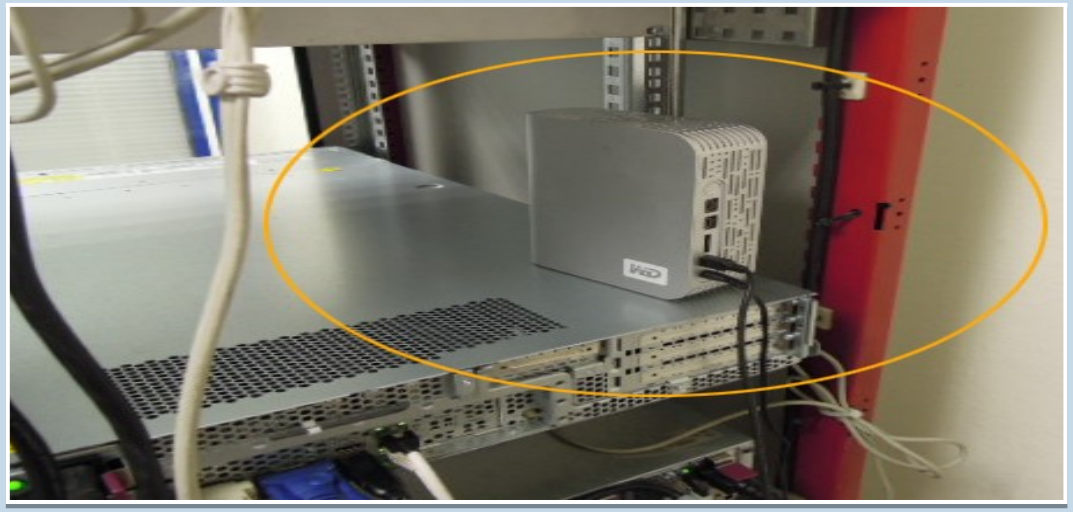
Uso del correo. No utilices tu cuenta de correo corporativa para usos personales, como apuntarte a páginas de viajes, ofertas… o enviar mensajes a amigos y familiares.



Trabaja en el Servidor

Almacena la información de forma segura y ayuda a conservarla. Guarda toda la información con la que trabajas en el servidor a través de la red informática, a fin de facilitar la realización de copias de seguridad y proteger el acceso frente a personas no autorizadas.

Pero no utilices indebidamente carpetas de red compartidas, los documentos sensibles no deben ser compartidos a través de dichas unidades, salvo en caso que máxima urgencia y cuando el emisor y receptor están previamente sincronizados.



Carpeta X

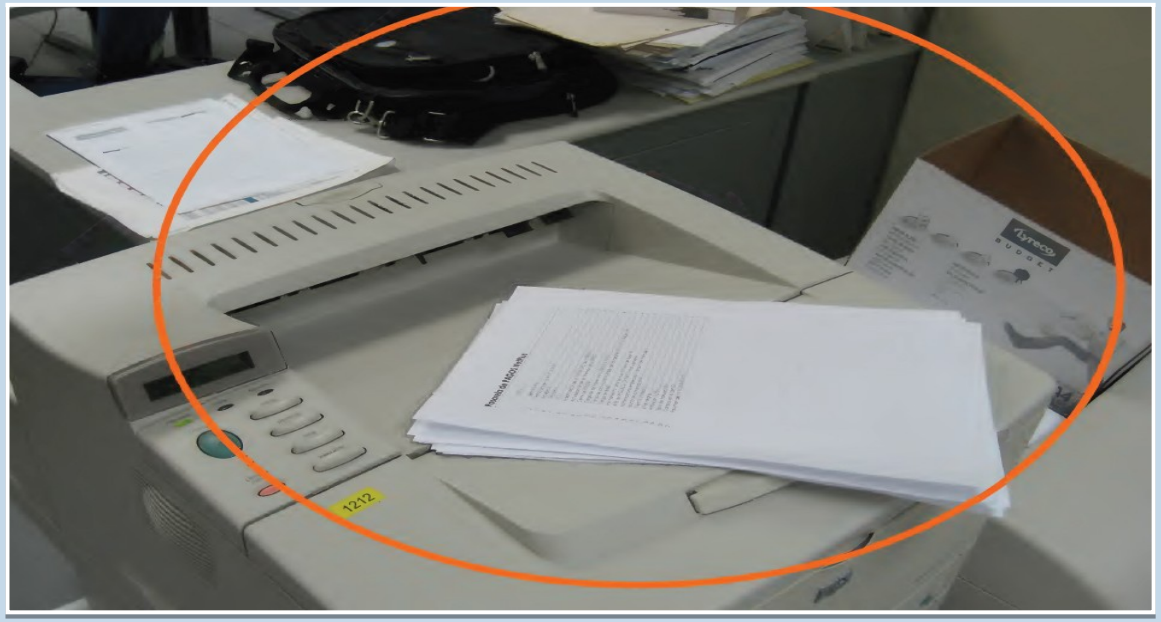
Dispositivos Móviles

No dejes nunca solos y sin atender tus dispositivos portátiles. Y de ser así, asegúralos guardándolos en un lugar seguro bajo llave o anclándolo a algo que no se puedan llevar.

Los móviles de empresa son dispositivos que requieren la misma seguridad que cualquier otro. Deben disponer de cifrado y antivirus, y recuerda activar el borrado remoto en caso de perdida o robo (o avisa inmediatamente al Departamento de Informática)

Información en papel

Se consciente de qué documentos compartes. Nunca dejes una copia de documentos confidenciales en sitios que puedan ser públicos o fácilmente accesibles.



Información en papel

Eliminar correctamente la documentación confidencial. Todos los documentos que contengan datos confidenciales y sobretodo aquellos que contengan información especialmente sensible, deben ser depositados en los contenedores confidenciales disponibles en la organización.

Información en papel

Cierre de despachos o dependencias. Mantén cerradas con llave todas aquellas dependencias a las que únicamente pueda acceder el personal autorizado, como despachos, el archivo, la sala de servidores, etc.

Custodia y almacenamiento de documentos. Mantén custodiado toda la documentación sensible que utilices, de forma que ninguna persona no autorizada pueda acceder a la misma. Cuando acabes con ella, archívala almacenándola debidamente según el criterio establecido.

Seguridad 365

Gracias

UOC
Universitat Oberta de Catalunya

UAB
Universitat Autònoma de Barcelona

UNIVERSITAT ROVIRA i VIRGILI

UIB
Universitat de les Illes Balears