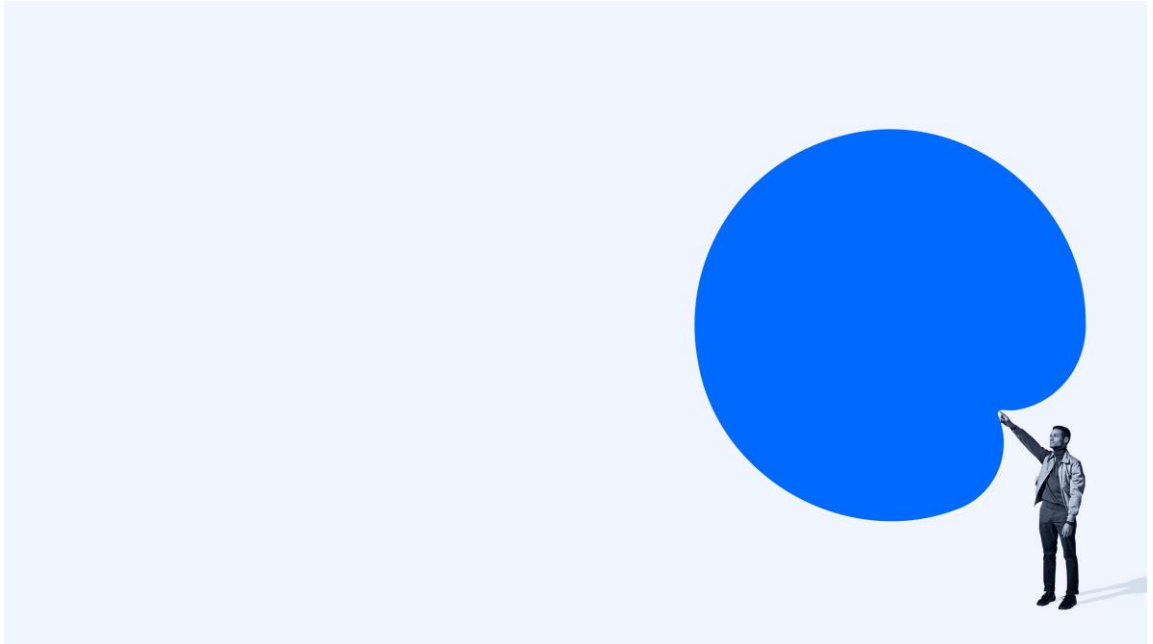
UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Área Jurídica y de Delegación de Protección de Datos

Telefónica Tech

FORMACIÓN: Protección de Datos Personales y Seguridad de la Información

14 Diciembre 2023



Área Jurídica y de Delegación de Protección de Datos

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Telefónica Tech

Impulsora del proyecto

Dª. Ana María Amorós

Directora Área Jurídica y de Delegación de Protección de Datos

Objeto de los Pliegos

- ✓ Seguimiento y adaptación RGPD
- ✓ Designación de un DPD
- ✓ Revisión y adaptación al ENS

Empresa adjudicataria

Telefónica-Tech

dpd@upv.es

servicio_juridico@upv.es

Gloria Martín – RGPD

Identificar las acciones necesarias para actualizar la implantación del RGPD y LOPD-GDD

Borja Sendra – DPD

Atención consultas y gestión de proyectos

SERVICIO PROTECCIÓN DE DATOS PERSONALES

Sumario

1. RGPD
2. Seguridad de la información
3. Conclusiones

Telefónica Tech

1. RGPD

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Contenido

1. Principios
2. Obligaciones
3. Derechos
4. Régimen sancionador

RGPD

01

PRINCIPIOS

QUÉ ES UN DATO PERSONAL

SÍ SON DATOS PERSONALES

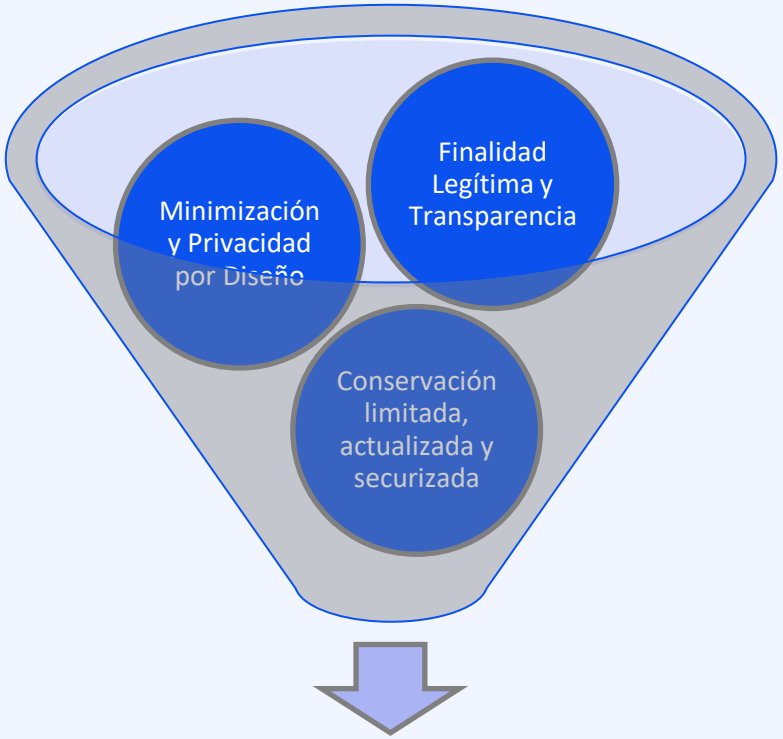
- Información de persona física identificada
- Información de persona identificable

NO SON DATOS PERSONALES:

- **Datos de PERSONAS JURÍDICAS**
  - Datos Registrales Públicos (CIF, dirección, etc.)
- **Datos de PERSONAS FALLECIDAS**
  - LOPDGDD: Derechos Familiares
  - Ley de Patrimonio Histórico

PRINCIPIOS - ¿Cómo debemos tratar los datos personales?

REGLAS DEL JUEGO



USO ADECUADO Y LÍCITO
DE LOS DATOS PERSONALES

RGPD

02

OBLIGACIONES

FINALIDAD CONCRETA Y LIMITADA

Foto de Glen Carrie en Unsplash

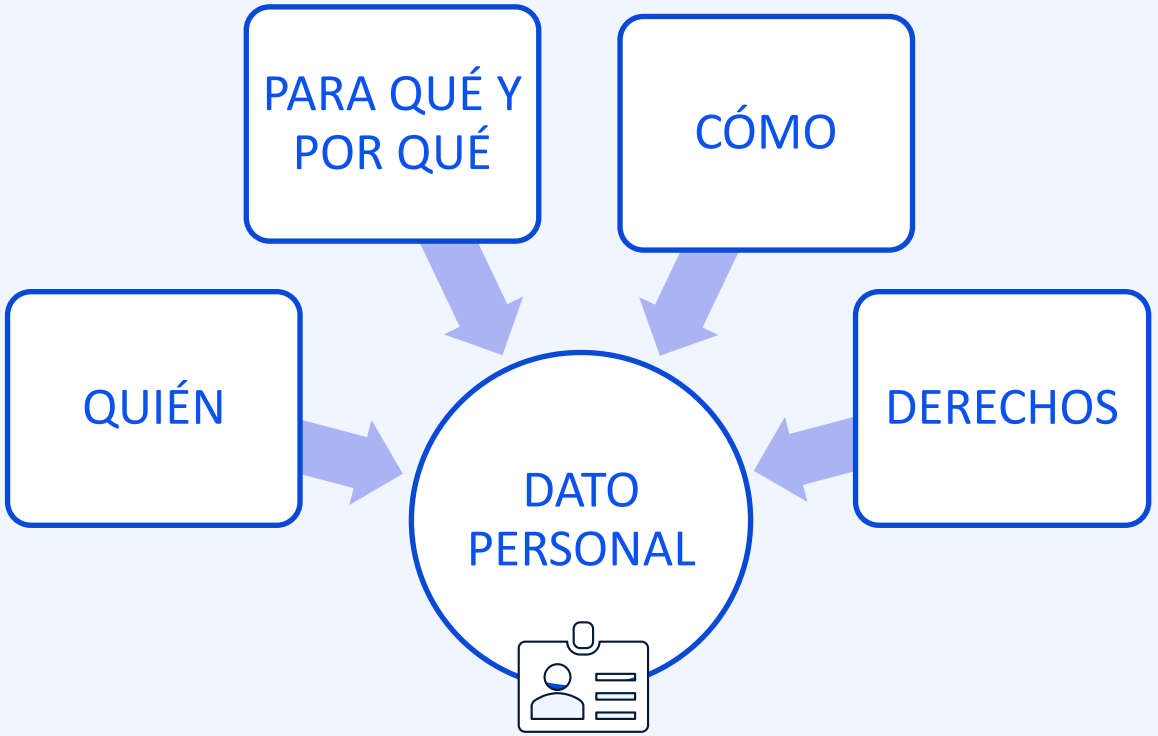
Recogemos los datos para una finalidad concreta

Usos posteriores

Excepciones: Consultar al DPD

DATOS ANONIMIZADOS: Posibilidad de Reutilización

Qué informar



Cuándo informar

Regla general

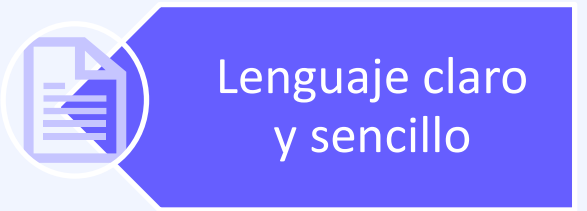
- RECOGIDA DE LOS DATOS

Excepción

- TAN PRONTO SEA POSIBLE DESDE LA RECEPCIÓN

TRANSPARENCIA

- Cuando recogemos datos personales, debe informarse de:
  - ✓ Datos de contacto de la UPV y del DPD
  - ✓ **La base jurídica para el tratamiento** (consentimiento, ejecución de un contrato; cumplimiento de una obligación legal; misión en interés público o ejercicio de Poderes públicos; interés legítimo del Responsable o un tercero)
  - ✓ **Categoria de destinatarios**
  - ✓ Informar de las **transferencias internacionales de datos.**
  - ✓ **Plazos o criterios de conservación de los datos.**
  - ✓ **Derechos y reclamación** ante la AEPD.



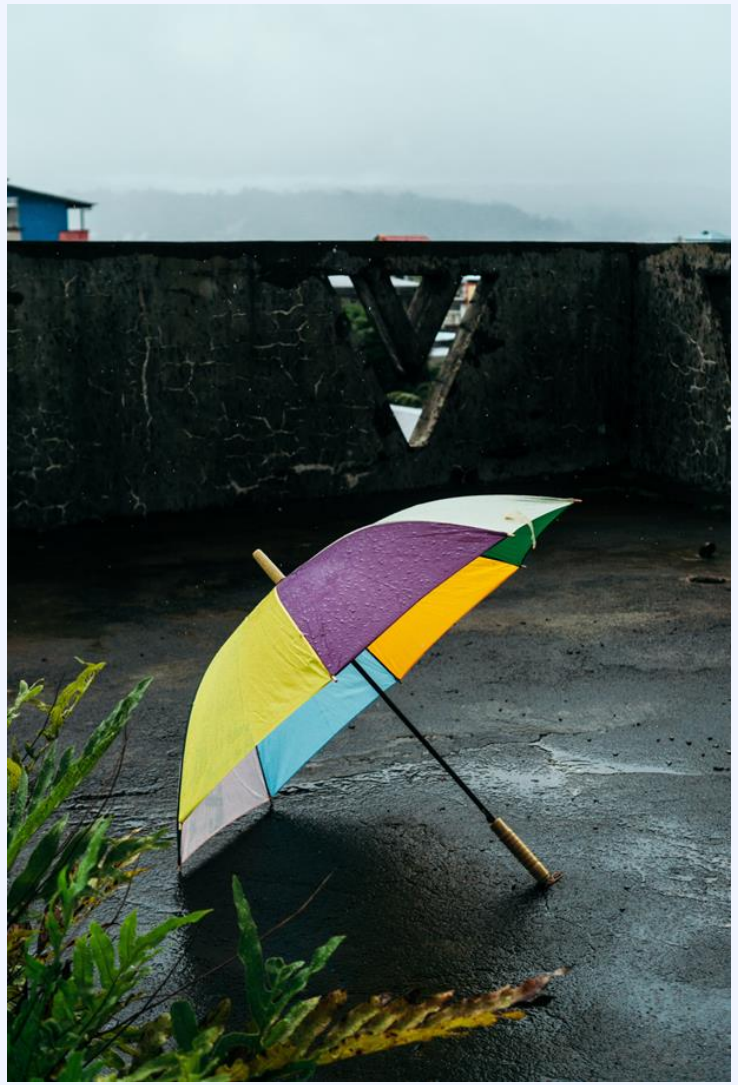
- Y, adicionalmente, en el caso de que los datos no se obtengan del propio interesado:
  - ✓ El **origen** o procedencia de los datos
  - ✓ Las **categorías o tipos de datos** (identificativos, características personales, etc.)

BASES DE LEGITIMACIÓN

- El tratamiento de los datos personales necesita una base legal que nos permita utilizarlos para una finalidad concreta:

  - ✓ Consentimiento informado del interesado
  - ✓ Aplicación de medidas contractuales o ejecución de un contrato en el que el interesado es parte
  - ✓ Cumplimiento de una obligación legal
  - ✓ Cumplimiento de una misión en interés público
  - ✓ Para proteger intereses vitales
  - ✓ Interés legítimo

- La mayoría de las actividades del tratamiento realizadas por la Universidad no requieren el consentimiento (salvo excepciones).



Excepciones: tratamientos que requieren consentimiento

EVENTOS

MENORES

DATOS SENSIBLES

¿Cómo debe ser el consentimiento?

Foto de Masjid MABA en Unsplash

- PREVIO
- INFORMADO
- SEPARADO
- DOCUMENTADO

MINIMIZACIÓN

Foto de Etienne Girardet en Unsplash

Solo recogemos los datos que necesitamos para la **finalidad**

Dato solicitado	Interesado
VIH	Candidatos
Embarazo	Candidatos
Antecedentes penales	Candidatos

Puesto de Personal Administrativo

Actor películas para adultos

Central Nuclear

Monitor de menores

Trabajos con sustancias peligrosas (laboratorios)

CASO DE ESTUDIO: Expediente Nº PS/00078/2021

Sanción a Hoteles por recogida del DNI

Divulgación de datos personales

REDES SOCIALES

TABLÓN DE ANUNCIOS

Foto de javier trueba en Unsplash

PUBLICACIÓN EN INTERNET DE LISTADOS

UNIVERSITAT POLITÈCNICA DE VALÈNCIA
SERVEI D'ALUMNAT

LISTADO DE PERSONAS ADMITIDAS Y EXCLUIDAS PARA SUBSANACIÓN DE DOCUMENTACIÓN DE LA CONVOCATORIA DE AYUDAS COMEDOR CURSO 2022-2023 FASE 1

Se procede a la publicación de la relación del estudiantado admitido y excluido de la Fase 1 tras la finalización del plazo de presentación de solicitudes, de acuerdo con el procedimiento indicado en la base 10ª de la Convocatoria.

Anexo I: Relación de personas excluidas
Anexo II: Relación de personas admitidas

En el Anexo I se relaciona el estudiantado que está excluido y el motivo de la exclusión.

Las personas interesadas podrán presentar las subsanaciones que consideren convenientes ante el motivo de su exclusión, en el siguiente plazo desde el **15 de septiembre de 2023** hasta el día **21 de septiembre de 2023, inclusive.**

Dichas subsanaciones se presentarán a través de la intranet apartado Secretaría Virtual/Solicitudes/Solicitudes de Becas

Esta admisión no supone la concesión de la beca. En breve se publicará la resolución provisional de la convocatoria, con la relación de beneficiarios y denegados, así como el plazo para presentar alegaciones a dicha resolución provisional.

En Valencia, a 14 de septiembre de 2023

Órgano Instructor Servicio de Alumnado

Consentimiento de los titulares o progenitores/tutores legales

Consentimiento NO necesario
Tiempo de publicación LIMITADO

Art. 28 RGPD

Elementos

Proveedores o terceros con **ACCESO A DATOS PERSONALES**

Se trata de cualquier tercero **que trate datos personales en nombre de la UPV** en virtud de un contrato u acuerdo.

Es necesaria la revisión por parte del DPD

REQUISITOS MÍNIMOS

CONSERVACIÓN DE LOS DATOS

TIEMPO LIMITADO

Foto de Nathan Dumlao en Unsplash

Los datos no pueden conservarse indefinidamente

ACTUALIZADOS

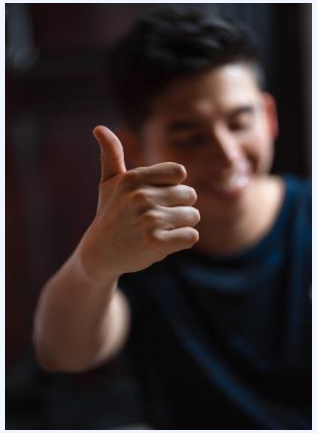


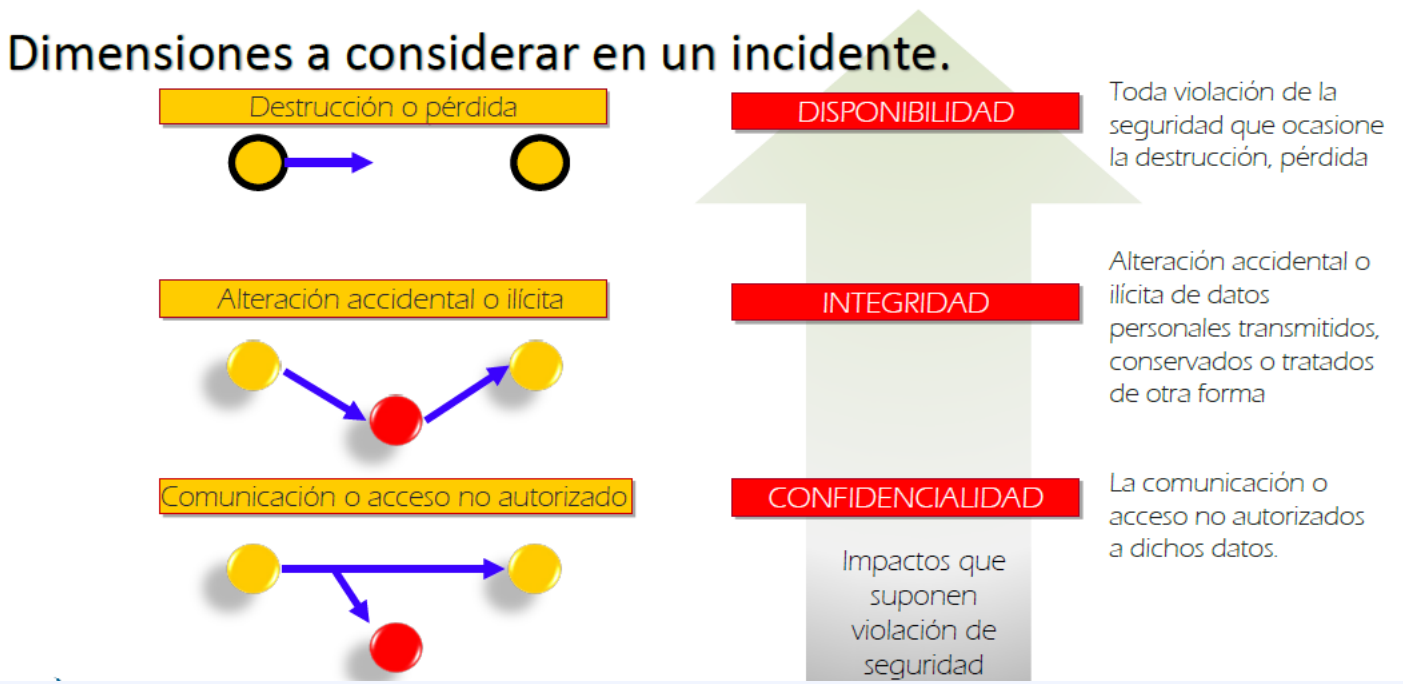
Foto de Johan Godínez en Unsplash

Los datos deben actualizarse durante el tiempo que los estemos usando para nuestra finalidad

SEGUROS

Los datos deben protegerse frente a accesos no autorizados de terceros

Art. 4.12. RGPD - Qué es una brecha de Seguridad



Destrucción, pérdida o alteración accidental o ilícita de los datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acción no autorizado de esos datos.

Art. 33 y 34 RGPD - Qué hago si detecto una brecha de seguridad

NOTIFICAR INMEDIATAMENTE al DPD y al ASIC:

- dpd@upv.es en caso de detectar que hay datos personales comprometidos.
- incidentes@upv.es en caso de detección de un incidente de seguridad.
- fraudeinternet@upv.es en caso de recepción de correo fraudulentos.

Aportar todos los datos conocidos: qué ha ocurrido, cómo ha ocurrido, qué sistemas se han podido ver afectados (ej: no acceso a aplicaciones concretas, al ordenador, etc.)

72 H notificar a la AEPD si existe riesgo para los derechos y libertados de los interesados

Ciberataque al Ayuntamiento de Sevilla

Página web y Sede electrónica afectada por un ransomware

Causa: falta de medidas de seguridad o error humano

Consecuencias: datos comprometidos y 72 h sin ofrecer servicio de sede electrónica a los ciudadanos

RGPD

03

DERECHOS

DERECHO DE ACCESO

Art. 15 RGPD

Qué debemos hacer

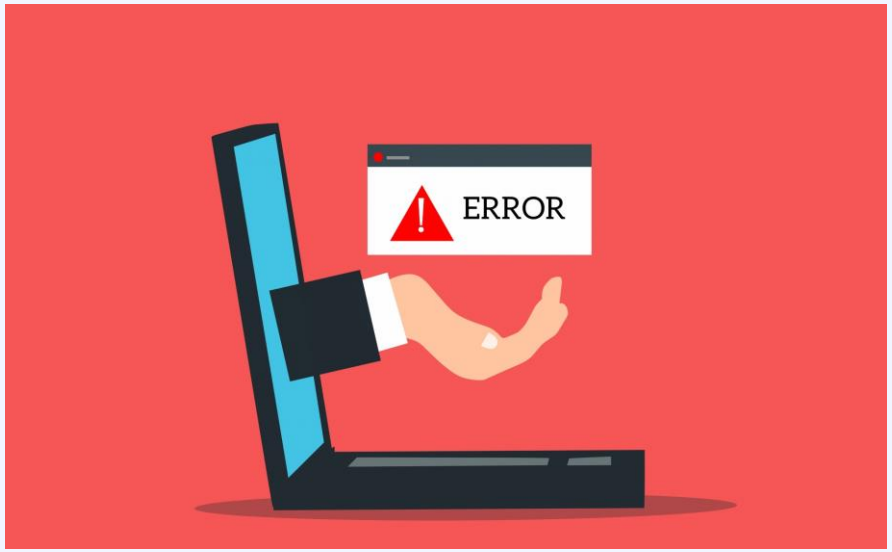
Si existe tratamiento de los datos…

INFORMAR Y ENTREGAR COPIA DE LOS DATOS

Finalidad
Categorías de datos tratados (datos de contacto, identificativos, de salud, etc.)
(terceros a los que le comunique los Destinatariosdatos)
Plazo que vamos a conservar los datos
Derechos
La existencia de decisiones automatizadas (en su caso)

DERECHO DE RECTIFICACIÓN

Art. 16 y 19 RGPD



Qué debemos hacer

Modificar los datos incorrectos, desactualizados o incompletos

NOTIFICAR a los TERCEROS a los que se hayan comunicado esos datos

DERECHO DE SUPRESIÓN

Art. 17 RGPD

Foto de Gary Chan en Unsplash

Qué debemos hacer

ELIMINAR si…

Datos innecesarios para la finalidad

Revocación del consentimiento

Oposición al tratamiento

Tratamiento ilícito

BLOQUEADOS (Conservados sin utilizarlos)
durante el tiempo de prescripción de reclamaciones o acciones legales

DERECHO AL OLVIDO

Art. 17 RGPD

Mario Costeja, el español que venció al todopoderoso Google

• Este gallego ha logrado que la Justicia Europea sentencie al buscador a eliminar datos que violen la ley de privacidad

Derecho frente a los buscadores de Internet (Google, Bing, Firefox, etc.)

EJEMPLO

CASO PRÁCTICO

1. **SUPUESTO:** Solicitante de empleo pide supresión de sus datos publicados en el Diari Oficial de la Generalitat Valenciana (BOP)**.**

2. **HECHOS:** La UPV no es responsable de las publicaciones que se realizan en el BOP y por lo tanto no puede proceder a su supresión, únicamente se podrá solicitar la rectificación.

3. **RECOMENDACIÓN:** Desestimar el derecho de supresión y recomendar ejercer el Derecho al Olvido frente al motor de búsqueda para desindexar el nombre del solicitante de la publicación realizada por el BOP.

DERECHO DE OPOSICIÓN

Art. 21 RGPD

Foto de Joshua Hoehne en Unsplash

Qué debemos hacer

DEJAR DE TRATAR LOS DATOS PARA ESA FINALIDAD

Cuando….

Exista una situación particular (art. 6.1.e) o f) RGPD)

Fines promocionales y de publicidad

Cómo…

EXCLUIR DATOS

Ejemplo

CASO PRÁCTICO 1

1. **SUPUESTO:** Se recibe solicitud de oposición por envío de ofertas de másteres y grados de la UPV.

2. **HECHOS:** El envío de estas comunicaciones se realiza en base al interés público de la universidad.

3. **SOLUCIÓN:** Cabe oposición del interesado y se detendrá el envío de estas comunicaciones con carácter inmediato.

CASO PRÁCTICO 2

1. **SUPUESTO:** Se recibe solicitud de oposición al tratamiento de videovigilancia realizado en la UPV.

2. **HECHOS:** Las grabaciones de videovigilancia se realizan en base al interés público de UPV en garantizar la seguridad de las personas e instalaciones.

3. **SOLUCIÓN:** No cabe oposición del interesado, puesto que, valorando sus intereses, predominan los de la UPV en cuanto a que pretende únicamente garantizar la seguridad.

ATENCIÓN DE DERECHOS

Foto de Steven Wright en Unsplash

Los Interesados quieren saber qué hacemos con sus datos

DPD atenderá las solicitudes
1 MES

Recibimos solicitudes → DPD **Dpd@upv.es**

RGPD

04

Régimen Sancionador

Qué ocurre si no cumplimos con nuestras obligaciones

Régimen sancionador de la AEPD y daños reputacionales

aepd agencia española protección datos

Buscar... Buscar | Sede electrónica | Preguntas frecuentes

Inicio | La Agencia | Derechos y deberes | Áreas de actuación | Publicaciones y resoluciones | Internacional | Prensa y actualidad

Áreas de actuación | Administraciones Públicas | Administraciones Públicas sancionadas por no responder a requerimientos y por incumplimiento de medidas

Administraciones Públicas sancionadas por no responder a requerimientos y por incumplimiento de medidas

- Canal prioritario
- Internet y redes sociales
- Reclamaciones de telecomunicaciones
- Publicidad no deseada

Última modificación: 5 de Septiembre de 2023

La Agencia Española de Protección de Datos ha venido observando como algunas Administraciones Públicas, principalmente las administraciones locales, no atienden, tal y como deberían, algunas de sus órdenes, lo que supone una infracción de la normativa de protección de datos.

Por este motivo, se ha querido destacar esta situación, incluyendo un nuevo apartado en la página web donde se muestran aquellas Administraciones Públicas que han sido sancionadas a lo largo de ese ejercicio por incumplimiento. Este incumplimiento es a una orden dada por la Agencia o por la falta de contestación a un requerimiento de petición de información en el marco de unas actuaciones previas de investigación.

ACCIÓN DE LA AEPD: Requerimiento, Sanción de apercibimiento

PRENSA: publicación en los medios de comunicación

Qué ocurre si no cumplimos con nuestras obligaciones

Art. 82 RGPD – Derecho a indemnización

Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del RGPD, tendrá derecho a recibir una indemnización por los daños y perjuicios sufridos

El TJUE admite que los daños no materiales por el uso ilícito de datos personales merecen una compensación económica

TJUE Rol N°C-300-2021.

Telefónica Tech

2. Seguridad de la Información
Buenas prácticas

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Contenido

1. ¿Qué hay de nuevo?
2. La lacra del malware
3. Ingeniería social
4. El puesto de trabajo

Seguridad de la Información

01

Qué hay de nuevo

1. ¿Qué hay de nuevo?

01

Julio 2023

Ciberdelincuentes usan reservas de hotel de Booking para robar datos de correos electrónicos

02

Julio 2023

El puerto más grande de Japón detiene sus operaciones por un ciberataque

03

Julio 2023

Suplantan a la Agencia Tributaria para introducir malware y robar tus datos bancarios

Seguridad de la Información

02

La lacra del malware

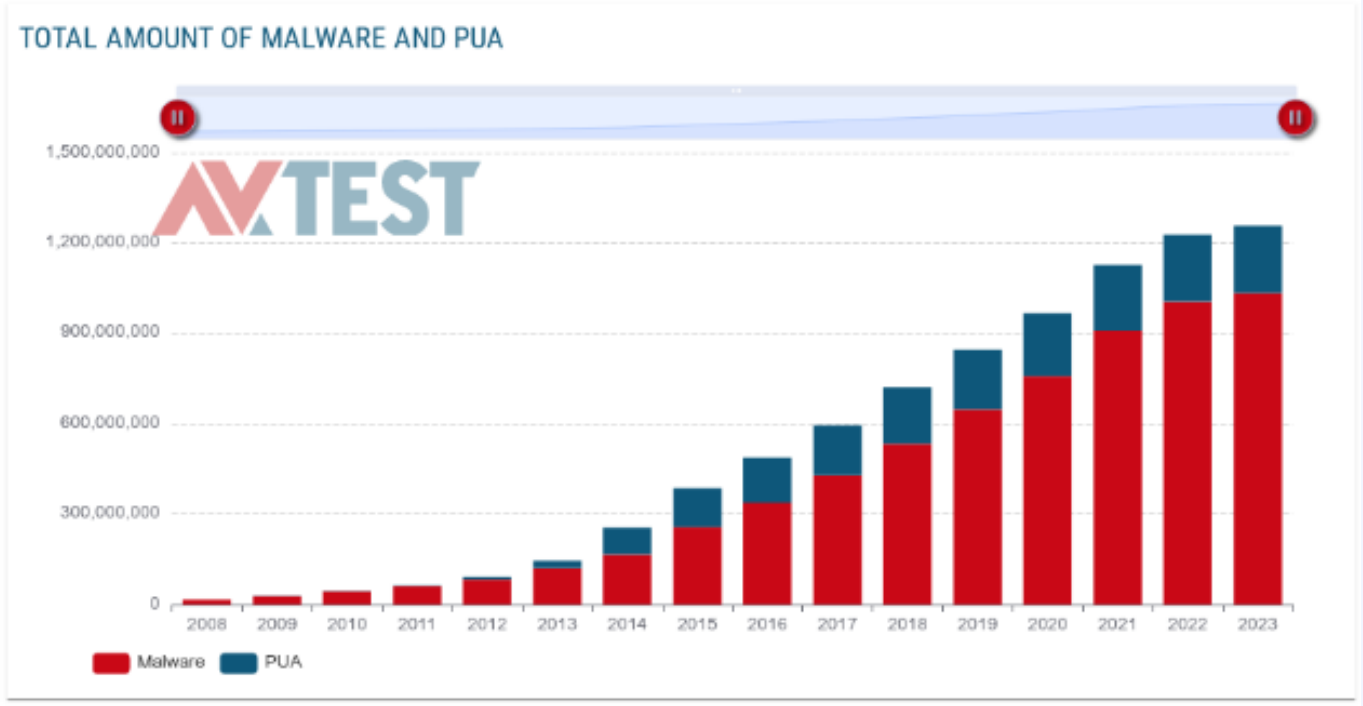
3. La lacra del malware

Programas cuya única misión es **infiltrarse** en un dispositivo sin el **conocimiento** ni **consentimiento** de su propietario para:

- ✓ Tomar el control del dispositivo.
- ✓ Robar información almacenada.
- ✓ Dañar datos.

2. La lacra del malware

Cantidad total de malware



Origen: av-atlas.org

2. La lacra del malware

TIPOS DE MALWARE

VIRUS	Alterar el correcto funcionamiento de un dispositivo.
SPYWARE	Recolectar información de forma no autorizada.
ADDWARE	Recolectar información de forma no autorizada con fines publicitarios o para comercializar con ella.
RANSOMWARE	secuestra los datos y pide un rescate por ellos.

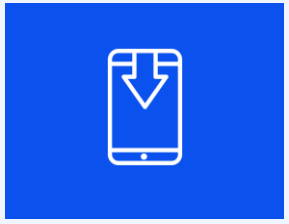
CIBERATAQUE

RansomHouse empieza a difundir datos robados del hospital Clínic

2. La lacra del malware

¿Cómo podemos prevenirlos?

Contar con un **antivirus actualizado** que proteja los equipos ante las principales amenazas de malware.



Mantener las **apps, programas y sistema operativo actualizados** (parches de seguridad).

Desinstalar programas y apps que ya no se utilicen (podrían ser utilizados como puerta de entrada de malware).

2. La lacra del malware

¿Cómo podemos prevenirlos?

Evitar ejecutar **ficheros o enlaces de origen desconocido**.

Descargar apps solo de las tiendas oficiales (Google Play en el caso de Android y Apple Store en iOS).

No conectar a equipos **USB desconocidos** (ataque por cebo).

2. La lacra del malware

¿Cómo podemos prevenirlos?

Estar al día en cuanto a amenazas de seguridad.

Realizar **copias de seguridad** ante posibles pérdidas de información.

Seguridad de la Información

03

Ingeniera Social

3. Ingeniería social

Ordenadores, tabletas, smartphones y televisores no solo están conectados a la red, sino también conectados con nosotros y entre ellos.

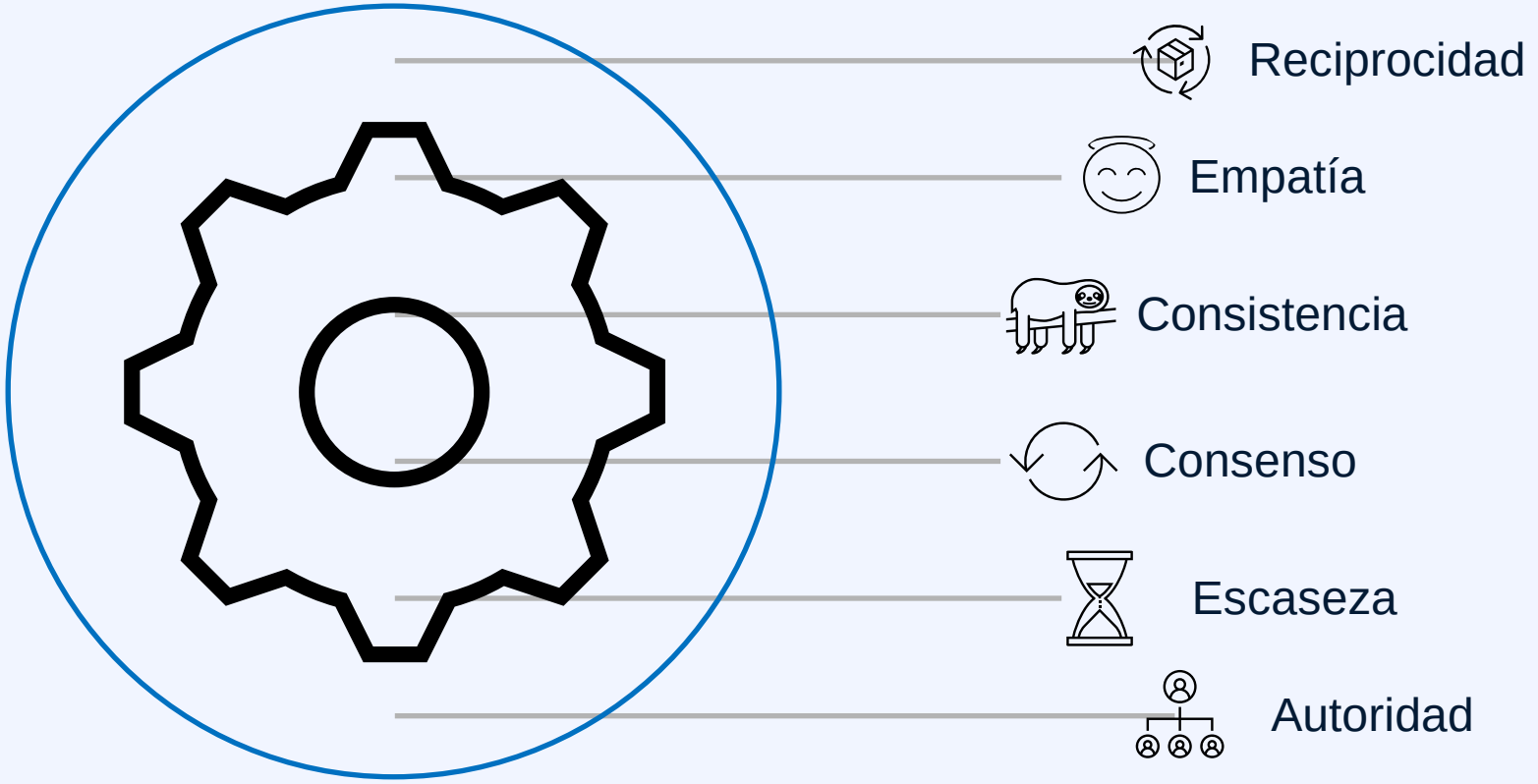
A través de ellos, gestionamos uno de los activos más valiosos con los que contamos: nuestra información y la información de terceros.

Esto, unido al uso masivo del correo electrónico, las redes sociales y las aplicaciones de mensajería instantánea, multiplican las oportunidades que tienen los ciberdelincuentes para llevar a cabo sus ataques.

3. Ingeniería social

¿Cómo lo hacen?

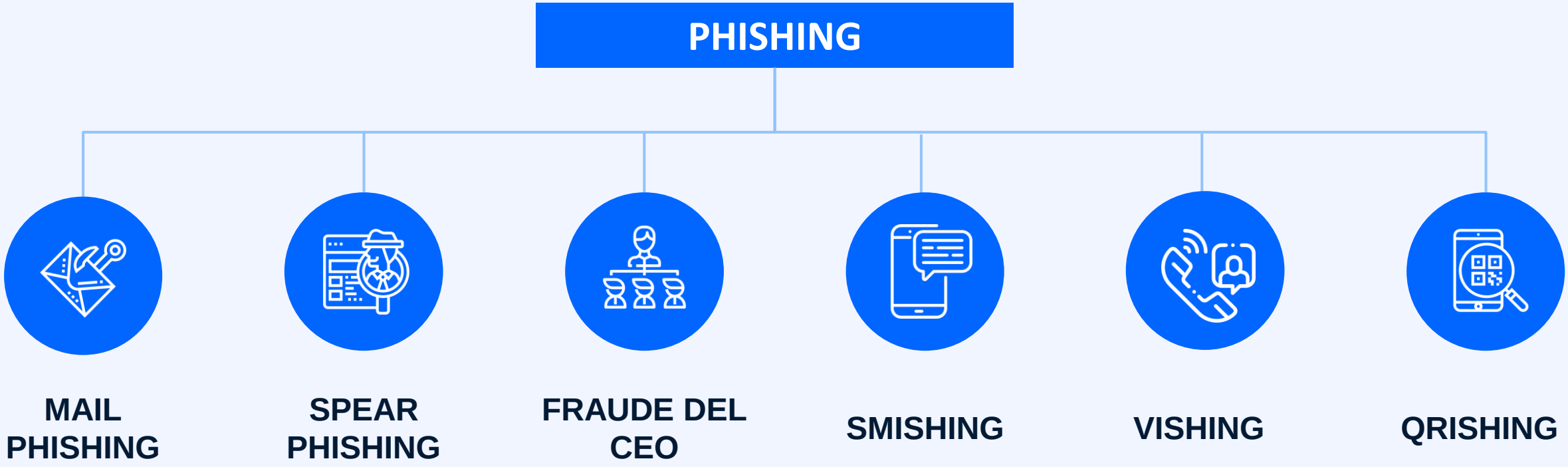
Utilizan infinidad de técnicas que podemos agrupar en los siguientes principios de actuación:



“Es más fácil manejar a las personas que a las máquinas”

3. Ingeniería social

Principales vectores de ataque por suplantación



3. Ingeniería social

Principales vectores de ataque por suplantación

PHISHING DEL CORREO ELECTRÓNICO

- Es el más usado por los ciberdelincuentes por su amplia capacidad de difusión y su variedad.
- Se le pide a la víctima que haga clic en un enlace, descargue un fichero o envíe una información para robársela, o infectar los dispositivos con *malware*.

De: Agencia Tributaria <gobierno@hacienda.gob.es>
Enviado: viernes, 25 de marzo de 2022 1:38
Para:
Asunto: Comprobante fiscal digital - MINISTERIO DE HACIENDA Y FUCION PUBLICA

Aviso de Notificaciones electrónicas

se anexa el seguiente comprobante fiscal digital Remitente: **Servicio de Administración Tributaria**. Hemos identificado que tienes pendiente de presentar, al 11 de Marzo de 2022, lo siguiente: **SERIE Y FOLIO: 398062**

A quien corresponda : **SERIE Y FOLIO: 398062** FECHA DE EMISION: 11/03/2022 **MONTO TOTAL: 6298.20**

SAT
Proveedores Autorizados de Comprobantes Fiscales Digitales

Descargar todo como.zip archivos adjuntos (236 kb)

3. Ingeniería social

Principales vectores de ataque por suplantación

3. Ingeniería social

Principales vectores de ataque por suplantación

SPEAR PHISHING

- ***Spear + phishing***: el phishing con arpón.
- El atacante se comunica con una víctima concreta, de la que ya tiene algún tipo de información recopilada, para engañarla y obtener información personal o corporativa.
- Al ser personalizados, las probabilidades de que nos genere confianza y nos fiemos, aumentan.

3. Ingeniería social

Principales vectores de ataque por suplantación

FRAUDE DEL CEO

- Normalmente a través del correo electrónico.
- El atacante suplanta a una persona de alto rango de la organización y se dirige una víctima a la que le pide ayuda para una operación confidencial y urgente.
- El objetivo es engañarla para que realice una o varias transferencias de importante cuantía, enmascaradas en una operación lícita y autorizada.

lun 14:25
Aurora
CONFIDENCIAL
Para Alfonso

Hola,

Te comunico que necesito que realizas el tratamiento de una operación financiera. ¿Podrías atenderme esta tarde con prioridad?

Atentamente.

Enviado desde mi iPhone

lun 14:32
Alfonso
RE: CONFIDENCIAL
Para Aurora

Por supuesto, Auri.

Cuenta conmigo absolutamente.
Ya me indicarás.

Un saludo,
Alfonso.

Enviado desde mi iPhone

lun 14:42
Aurora
RE: CONFIDENCIAL
Para Alfonso

Perfecto, Alfonso.

Estamos en este momento efectuando una operación financiera en relación a la compra de maquinara para la empresa. Esta operación debe ser estrictamente confidencial, y te obliga a no hablar de esto con nadie de momento en la empresa, ni por teléfono ni por voz.

El anuncio legal de esta adquisición será entre el 12 y el 15 de febrero de 2019, en nuestras instalaciones.

Para finalizar, necesito que me indiques el saldo con el que contamos y el número de cuenta.

Atentamente.

Enviado desde mi iPhone

3. Ingeniería social

Principales vectores de ataque por suplantación

SMISHING

- ***SMS + phishing***: el phishing de los mensajes de texto.
- El ciberatacante se vale de técnicas de engaño a través de la mensajería de texto para conseguir información del usuario y hacer un uso fraudulento de ella.
- Promociones irresistibles, avisos de mensajería de transporte o logística o información de nuestra entidad bancaria son los más utilizados.

3. Ingeniería social

Principales vectores de ataque por suplantación

VISHING

- ***Voice + phishing***: el phishing de la llamada.
- El atacante contacta por teléfono con la víctima para manipularla con alguna treta o excusa y que revele información sensible de cualquier tipo.
- Para disfrazar su identidad real, pueden utilizar protocolos VoIP (programas de suplantación de los sistemas de identificación de llamadas) o software de modificación de voz).

3. Ingeniería social

Principales vectores de ataque por suplantación

QRISHING

- ***QR + phishing***: el phishing del QR
- Al escanear un código QR, la víctima es dirigida a una web fraudulenta, donde se le piden credenciales, datos u otra información sensible.
- Ante la imposibilidad de distinguir la veracidad o no del QR a simple vista, el delincuente se aprovecha de la confianza de los usuarios.

3. Ingeniería social

¿Cómo podemos detectarlo?

Analiza el remitente

Direcciones que no se corresponden con el presunto remitente del correo electrónico.

Expresiones impersonales

Uso de frases como *Estimado cliente*, *Querido colaborador*, *Sr* o *Sra*…para dirigirse a nostros.

Revisión de sus datos maestros

BS Banco S.A <info@autovisual.com>
Para

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Santander

Estimado Cliente,

Asunto : Su tarjeta será suspendida !
Remitente : Servicio al cliente.

Estamos teniendo problemas para verificar la información de su tarjeta.
Lo invitamos a corregir este problema haciendo clic en el enlace de abajo y siguiendo las instrucciones :

https://www.bancosantander.es/es/particulares

Este es un mensaje automático. Gracias por confiar en nosotros.

3. Ingeniería social

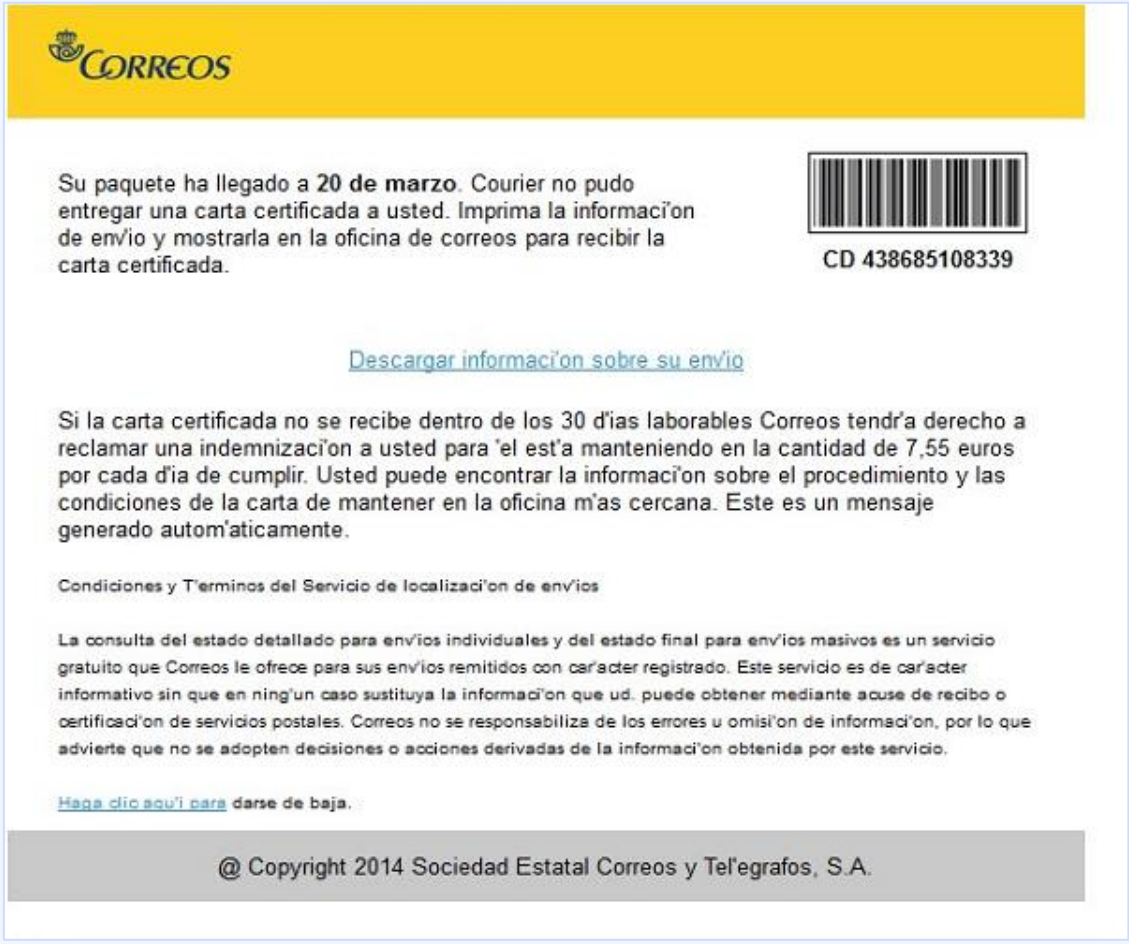
¿Cómo podemos detectarlo?

Errores ortográficos o gramaticales

Traducciones sospechosas o con simbología extraña en el cuerpo del mensaje suponen claro síntoma de fraude.

Redirección a otras webs

Los enlaces sospechosos (http en vez de HTTPS o dominios desconocidos) y con presencia de caracteres extraños ($, %, &…) deben activar nuestras alarmas.



CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 438685108339

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede obtener mediante acuse de recibo o certificaci'on de servicios postales. Correos no se responsabiliza de los errores u omisi'on de informaci'on, por lo que advierte que no se adopten decisiones o acciones derivadas de la informaci'on obtenida por este servicio.

Haga clic aqu'i para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Tel'egrafos, S.A.

3. Ingeniería social

¿Cómo podemos detectarlo?

De: AgenciaTributaria [mailto:noreplys1@eagenciatributaria.es]
Expuesto a las: martes, 28 de mayo de 2019 10:18
Expuesto en: [redacted]
Conversación: Reembolso del impuesto en valor....
Asunto: Reembolso del impuesto en valor....

GOBIERNO DE ESPAÑA

Estimado contribuyente,

Mandamos este e-mail para dar a conocer lo siguiente:
Después del último cálculo sobre las actividades fiscales, hemos decidido que le coresponde un reembolso del impuesto en valor de 512,19 €.

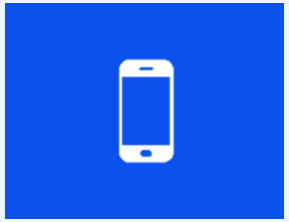
Para recibir dicho reembolso, completar y mandar el formulario del impuesto a devolver.

Pulsar aqui para acceder al reembolso. »

3. Ingeniería social

¿Cómo podemos prevenirlos?

Evita clicar en ningún enlace sin revisar primero con detenimiento su URL y en ningún caso accedas a sitios web que no comiencen por **HTTPS**.

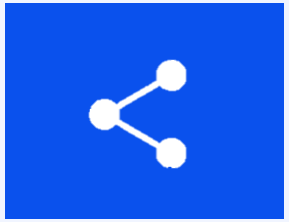


Desconfía de todos aquellos **mensajes** y **llamadas** que recibas por cualquier medio y cuya procedencia sea **desconocida**, más aún cuando te soliciten información privada o sensible.

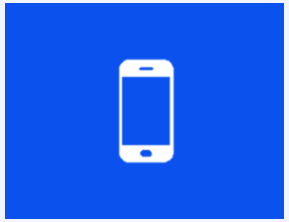
No **instales** por tu cuenta programas o **aplicaciones** de sitios web no oficiales o de dudosa reputación, y en ningún caso cuando no hayan sido **debidamente aprobados** por la entidad.

3. Ingeniería social

¿Cómo podemos prevenirlos?



Sé **precavido** a la hora de **compartir información** en **RRSS**. Los ciberatacantes las utilizan para recopilar datos y utilizarlos contra nosotros.



No utilices en ningún caso tus **dispositivos** o equipos **corporativos** para **fines personales**, ni viceversa. La información laboral siempre es sensible y que se vea comprometida puede resultar fatal.

Sospecha de **correos** o **SMS mal redactados** o que recojan un contenido demasiado bueno para ser cierto. No abras **adjuntos sospechosos** o desconocidos.

3. Ingeniería social

¿Cómo podemos prevenirlos?

Protege tus **credenciales** de **acceso**: son la primera línea de defensa contra los atacantes. Recuerda que son personales e intransferibles y solo tú debes hacer uso de ellas.

Utiliza **contraseñas robustas**: con una longitud suficiente, que contengan letras mayúsculas y minúsculas, números y caracteres especiales. Que sean **diferentes** para cada servicio y **actualízalas** periódicamente.

Utiliza el sistema de **conexión VPN** para acceder a los recursos corporativos, añadiendo una capa de **seguridad** que proteja la información de la organización.

3. Ingeniería social

¿Cómo podemos prevenirlos?

Elimina la **información sensible** de tus dispositivos siempre que acabes de utilizarla, y utiliza para ello sistemas de **borrado seguro** habilitados a tal efecto.

Evita conectarte a **redes Wifi Públicas**, como las de aeropuertos, hoteles y centros comerciales, siempre que no sea estrictamente necesario.

Y lo **más importante**, ante la menor duda o sospecha de haber caído en un fraude o detectar el funcionamiento errático de alguno de tus dispositivos, no dudes en **contactar con el departamento de informática.**

Seguridad de la Información

04

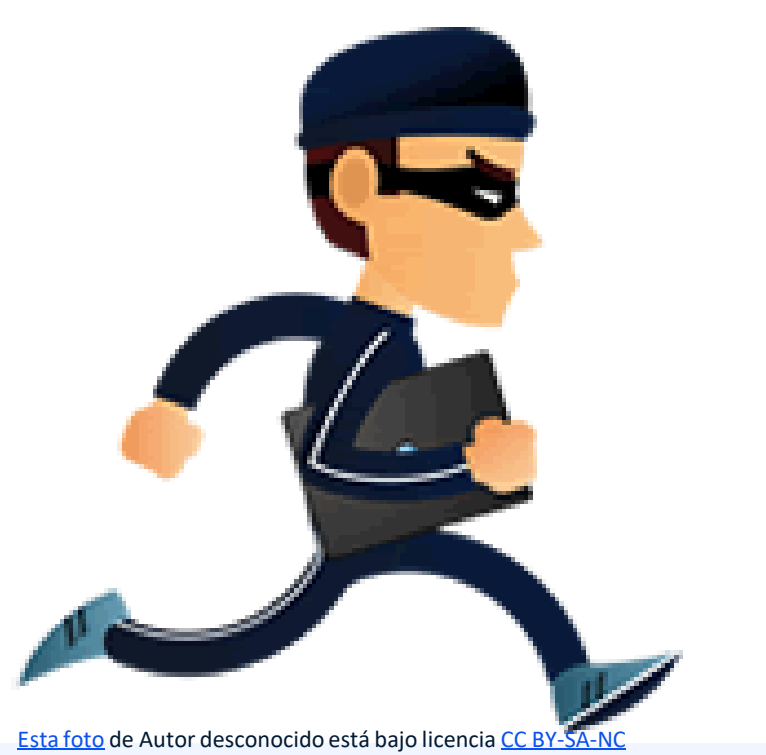
El puesto de trabajo

4. Protege los sistemas de información

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

4. Protege los dispositivos móviles



No dejes nunca solos y sin atender tus dispositivos portátiles en lugares públicos o entornos poco fiables

Asegúralos guardándolos en un lugar seguro bajo llave o anclándolo a algo que no se puedan llevar.

En caso de pérdida o robo recuerda avisar inmediatamente al ASIC.

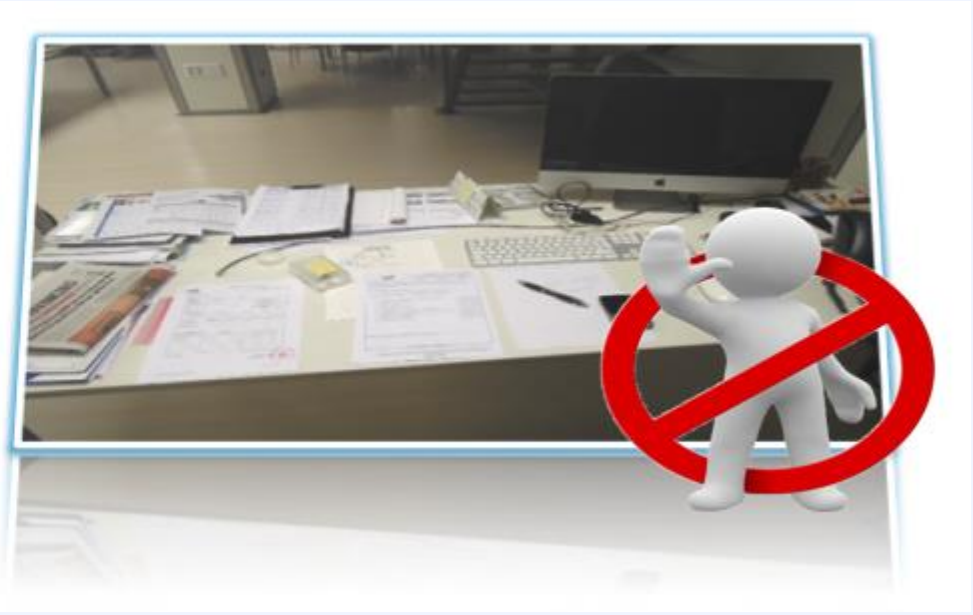
4. Uso responsable de los sistemas de información

Foto de Nadine Shaabana en Unsplash

- Utiliza los soportes y equipo que te facilita la corporación de forma responsable.
- No alteres la configuración física o lógica de los equipos.
- No instales software no autorizado.
- No utilices soportes portátiles en equipos no confiables o poco seguros.
- No extraigas información sin autorización.
- Utiliza la CCOO para el envío de emails masivos

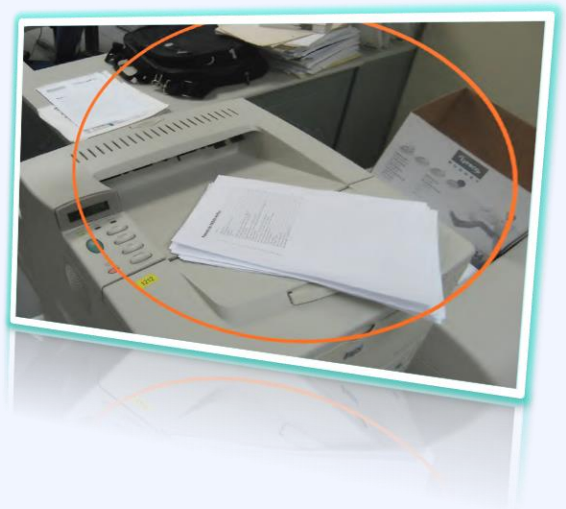
4. Mesas limpias

No dejes papeles con información personal en la mesa cuando te ausentes



4. Protege la información en papel

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



Elimina correctamente la documentación confidencial. Todos los documentos que contengan datos confidenciales y sobre todo aquellos que contengan información especialmente sensible, deben ser depositados en los contenedores confidenciales disponibles en la entidad.

Telefónica Tech

3. Conclusiones

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Principales ideas

1. Utilizar los datos personales aplicando los principios – **Reglas del juego**

2. Sigue el procedimiento de **Atención de Derechos**

3. **Notifica inmediatamente al DPD y al ASIC cualquier incidente de seguridad que pueda afectar a datos personales** (accesos no permitidos, robo de móviles, ordenadores de trabajo, contraseñas, etc.).

4. **Aplicar buenas prácticas en la protección de la información**

Telefónica Tech

Muchas gracias

UNIVERSITAT POLITÈCNICA DE VALÈNCIA