Formación en seguridad de la información

universidad de león

1.Seguridad de la información en las AAPP

- El Esquema Nacional de Seguridad (ENS) establece una política de seguridad en el uso de medios electrónicos en las Administraciones públicas y se constituye mediante unos requisitos que permiten la protección de la información
- El marco normativo por el que se rige el ENS aparece comprendido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica
- Tiene por finalidad el asegurar la confianza en el uso de medios electrónicos, mediante una serie de garantías en la seguridad de los datos, las comunicaciones y los servicios electrónicos
- Las Administraciones públicas, para garantizar los principios básicos de acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, servicios e información en los medios electrónicos, aplican el ENS
- Por tanto, el ENS también será de aplicación a los ciudadanos en sus relaciones con las Administraciones públicas, se aplicarán también a las propias Administraciones públicas, y a las relaciones entre distintas Administraciones públicas

Principios básicos

- Las decisiones de seguridad, en el ENS, tiene como principios básicos:
  - La **seguridad como proceso integral** que consiste en un proceso constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema, dando la máxima atención a la concienciación de las personas intervinientes en el proceso.
  - **Gestión de la seguridad basada en los riesgos**. El análisis y gestión de los riesgos es la parte esencial del proceso de seguridad y deberá estar permanentemente actualizado, lo cual permitirá un mantenimiento del entorno, minimizando los riesgos hasta unos niveles aceptables mediante medidas de seguridad.
  - **La prevención, detección, respuesta y conservación** son parte esencial ya que nos permiten impedir que la amenaza se materialice y no afecte gravemente a la información.
  - Existencia de **líneas de defensa**, sirven para establecer una estrategia de protección mediante capas, de manera que, en caso de fallo de una capa, esto nos permita ya sea ganar tiempo de reacción ante el incidente, reducir la posibilidad de comprometer el sistema en su conjunto y minimizar el impacto final, siendo estas medidas de defensa de naturaleza tanto física, organizativa como lógica.
  - **Vigilancia continua**
  - **Reevaluación periódica**. Estas medidas de seguridad han de reevaluarse periódicamente para adaptarlas a la evolución de los riesgos y sistemas de protección.
  - **Diferenciación de responsabilidades**. En los sistemas de información, hemos de diferenciar al responsable de la información, del responsable del servicio, del responsable de seguridad.

Requisitos mínimos en el ENS

- Los requisitos mínimos, de obligado cumplimiento, son las exigencias necesarias para asegurar la información y los servicios.
  - a) Organización e implantación del proceso de seguridad.
  - b) Análisis y gestión de los riesgos.
  - c) Gestión de personal.
  - d) Profesionalidad.
  - e) Autorización y control de accesos.
  - f) Protección de las instalaciones.
  - g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
  - h) Mínimo privilegio.
  - i) Integridad y actualización del sistema.
  - j) Protección de la información almacenada y en tránsito.
  - k) Prevención ante otros sistemas de información interconectados.
  - l) Registro de la actividad y detección de código dañino.
  - m) Incidentes de seguridad.
  - n) Continuidad de la actividad.
  - ñ) Mejora continua del proceso de seguridad

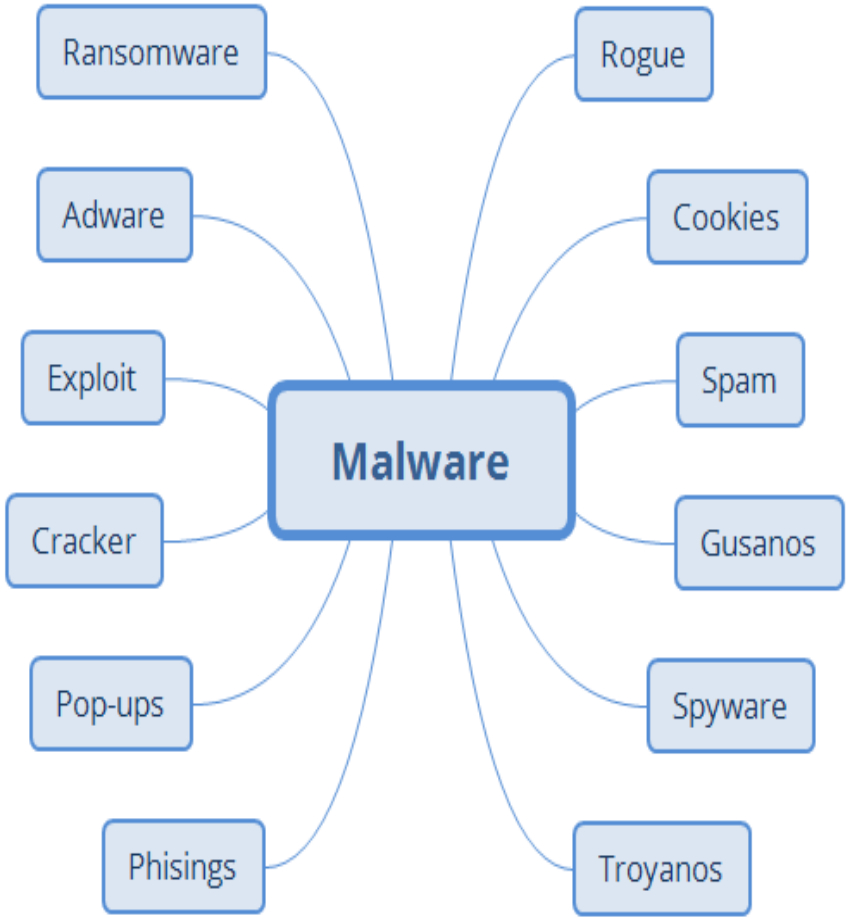
ENS 2010

- **Principios básicos:** prevención, reacción y recuperación.
- No existía el principio básico de **Vigilancia continua**.
- Menor visibilidad al **componente certificado** de hardware y software.
- **Requisitos**: seguridad por defecto.
- No existía el servicio en la nube en las medidas del marco operacional.
- **4** marcos organizativos.
- **31** marcos operacionales.
- **40** medidas de protección.
- **Refuerzos** en los mecanismos de autenticación.

ENS 2022

- **Principios básicos:** prevención, detección, respuesta y conservación.
- Se introduce el principio básico de **Vigilancia continua** (auditoría obligatoria anualmente).
- Máxima importancia **componente certificado** de hardware y software.
- **Requisitos**: mínimo privilegio (modificación de terminología).
- Nueva familia de medidas del marco operacional: **servicio en la nube.**
- **4** marcos organizativos (se mantiene el número).
- **33** marcos operacionales (aumentan 2 marcos).
- **36** medidas de protección (se reducen 4 marcos).
- Mayores **refuerzos** en los mecanismos de autenticación.

2.SOFTWARE MALICIOSO



- Al Software Malicioso se le conoce por el término Malware.
- el término **Malware** es el término principal empleado por los profesionales de la informática para referirse a todas aquellas amenazas de carácter informático.
- distinguirlo del **software defectuoso**

¿Cuál es el propósito de un Malware?

- Robo de información
- Secuestro
- “Reclutamiento” para una red de bots

Principales tipos de ataques malware

- **Virus informático**→ programas maliciosos que afectan a otros archivos del sistema con la intención de modificarlos o dañarlos.
- **Gusano informático** → su principal diferencia respecto de los virus informáticos es que **no necesita la intervención del usuario ni la modificación de ninguno de los archivos** existentes para infectar un equipo.
- **Troyano**→ busca ejecutar acciones ocultas con las que abrir una puerta trasera.
- **Spyware**→ busca recolectar información sobre un usuario u organización sin el conocimiento o el consentimiento del propietario del equipo
- **Ransomware** → busca cifrar la información contenida en el equipo y exigir a cambio de la contraseña a un rescate.
- **Rootkits**→ Este software funciona como una puerta trasera, para que un malware entre y cause estragos dentro del sistema.
- **Keyloggers** → almacenan la información recopilada y la envían al atacante, el cual puede extraer información delicada tal como el nombre de usuario y contraseñas, así como detalles de tarjetas de crédito

¿Cómo detectar un malware?

- Funcionamiento lento o mal funcionamiento.
- Se muestran mensajes de error repetidamente.
- No se puede apagar el dispositivo o no se puede reiniciar.
- Aparecen en pantalla un montón de ventanas pop-up.
- Aparecen en pantalla anuncios inapropiados o anuncios que interfieren con el contenido de la página.
- El equipo no permite eliminar un programa indeseado.
- Aparecen anuncios en lugares atípicos, por ejemplo, en sitios web del gobierno.
- Se envían mensajes de correo electrónico que el usuario no escribió.
- El navegador web redirecciona automáticamente a una página web que no ha sido solicitada por el usuario.
- Se bloquean los accesos a páginas web de actualizaciones del sistema y de los programas de protección del equipo como antivirus y anti malware.

Principales vías de infección de malware

- Redes sociales
- Sitios web fraudulentos
- Programas “gratuitos”, la mayoría de ellos se encuentran infectados y contienen cualquier tipo de malware
- Dispositivos USB/CDs/DVDs infectados
- Sitios web legítimos previamente infectados
- Archivos adjuntos en correos no solicitados (Spam)

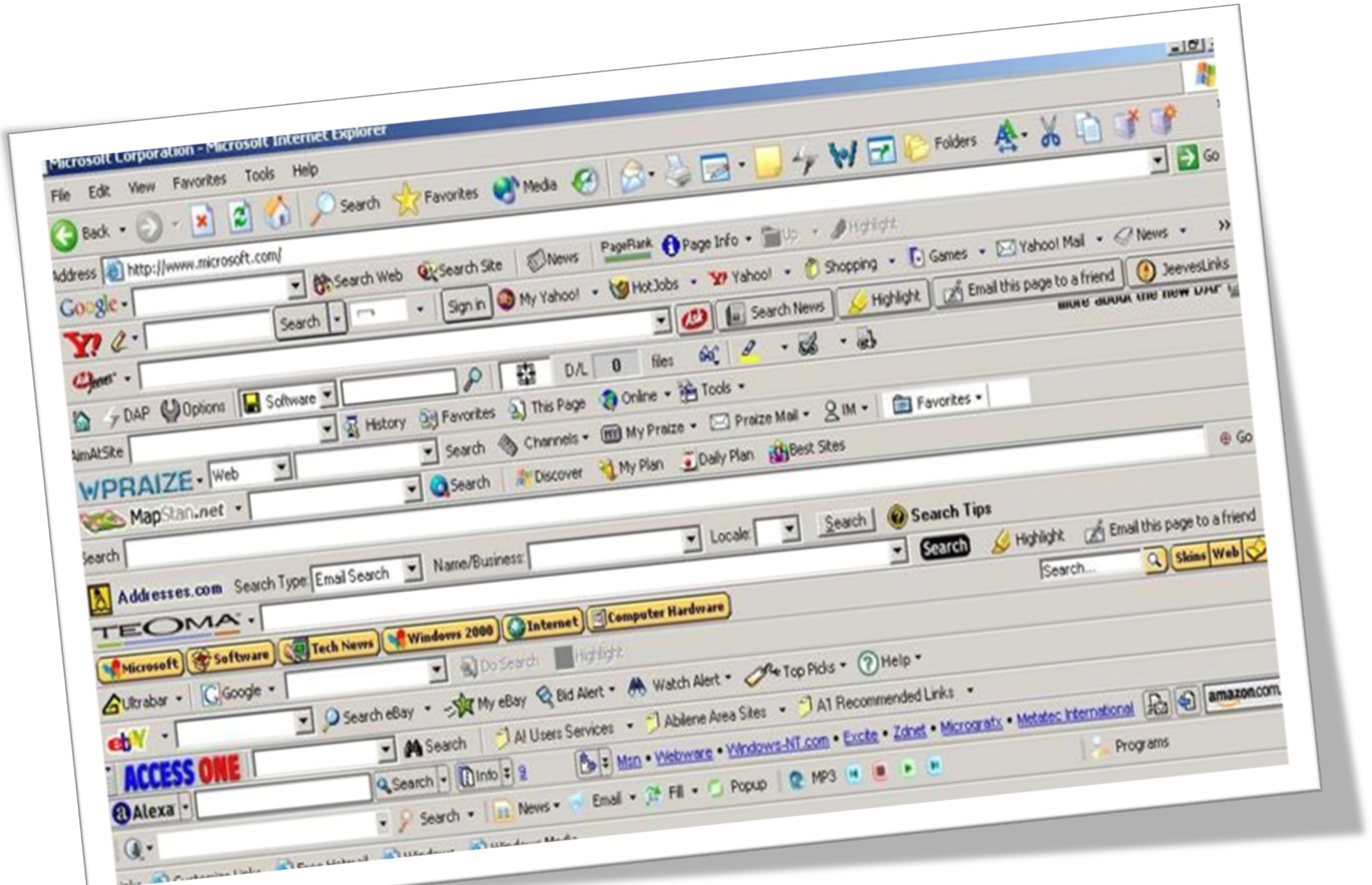
¿Qué hacer si detecta un Malware?

- **Dejar inmediatamente de realizar compras, trámites bancarios y cualquier otra actividad online** que involucre nombres de usuario, contraseñas o cualquier otra información delicada.
- **Actualizar el software de seguridad (antivirus) y realizar un escaneo completo del equipo** para controlar si detecta algún tipo de malware. Además se debe **eliminar todo aquello que aparezca identificado como problemático**. Una vez aplicados estos cambios se debe reiniciar el equipo.
- Se debe **restablecer la configuración original del navegador web**.
- En el caso de que el equipo esté cubierto aún por una garantía que le ofrece un servicio de soporte técnico gratuito, se debe **contactar con el fabricante**

Recomendaciones para prevenir un Malware

- Instalar todos los **parches y actualizaciones** del Sistema Operativo.
- Usar un navegador de Internet moderno y **actualizado.**
- Instalar todas las **actualizaciones** de Java, Adobe flash y otras librerías de internet, en el mismo momento en que se produce la actualización.
- Tener siempre funcionando en segundo plano un **antivirus** y un **cortafuegos** actualizados.
- Realizar **comprobaciones periódicas** con algún programa especializado en troyanos y gusanos.
- No abrir correos de **fuentes desconocidas** ni acceder a webs de mala reputación.
- Al descargar un archivo dudoso, antes de usarlo comprobarlo con un **antivirus.**
- **No modificar la configuración** de seguridad que viene por defecto en el navegador web, se puede minimizar las descargas “drive-by” o empaquetadas.
- Se debe prestar atención a las **advertencias de seguridad** del navegador web, muchos navegadores tienen incorporada una función de escaneo de seguridad que mostrará un mensaje de advertencia antes de visitar una página web infectada o de descargar un archivo malicioso.
- En lugar de hacer clic en el enlace de un email, se debe escribir **directamente el URL** de un sitio web confiable en la barra de su navegador. Los delincuentes envían emails que parecen enviados por compañías conocidas y confiables. Los enlaces tal vez parezcan legítimos, pero al hacer clic pueden instalar un software malicioso en el dispositivo o dirigir al usuario a un sitio web fraudulento.
- No se debe hacer clic en las ventanas **pop-up** ni en los carteles de los **anuncios** con información sobre el rendimiento del ordenador. Los estafadores insertan programas maliciosos en carteles de anuncios que lucen legítimos, especialmente en los anuncios que hacen referencia al funcionamiento del ordenador. Si no se conoce la fuente de esos anuncios, se debe evitar hacer clic.
- Se deben **escanear** las unidades de memoria USB y demás dispositivos externos antes de usarlos. Estos dispositivos pueden estar infectados con software malicioso, especialmente si se usan en lugares muy concurridos, como kioscos de impresión de fotografías u ordenadores de uso público.
- Se deben hacer **copias de seguridad** con regularidad.
- Los **usuarios** deberían mantenerse medianamente **informados** sobre la aparición de nuevas amenazas.

3.PROGRAMAS Y ARCHIVOS POTENCIALMENTE NO DESEADOS



¿Por qué se llama PUP y no malware?

- el usuario otorga su consentimiento para descargarlo
- cláusulas demasiado escondidas o enrevesadas como para ser fácilmente encontradas por los usuarios
- estos programas no son catalogados como malware
- un antivirus se arriesga a que la empresa de software o el desarrollador le ponga una demanda

Tipos de PUP

- Barras de herramientas (toolbars)
- Programas que modifican configuraciones de navegadores de Internet.
- Instaladores (o “software wrappers”) que se comportan como parásito
- Aplicaciones que son distribuidas mediante el modelo de negocio “pagar por instalar” (pay-per-install).

Síntomas de infección PUP

- Los banners publicitarios se inyectan con las páginas web que está visitando.
- El texto de la página web aleatoria se convierte en hipervínculos.
- Aparecerán ventanas emergentes del navegador que recomiendan actualizaciones falsas u otro software.
- Otros programas publicitarios no deseados pueden instalarse sin que el usuario lo sepa.

¿Cómo protegerse de los PUP?

¿Qué son los archivos potencialmente no deseados?

Fuente	Descripción
Instalaciones de Software	Cuando se instala software en el equipo, el proceso de instalación crea archivos temporales como parte del proceso. En algunos casos, el instalador no limpia estos archivos temporales al finalizar la instalación.
Navegación por Internet	Cuando se navega en una página web, el navegador descarga el texto y los gráficos que forman el contenido de la página. Cuando se termina de ver la página, el navegador puede dejar el contenido que descargó en el equipo. El contenido que se descargó ayuda a mostrar la página web con mayor rapidez cuando el usuario vuelva a visitar la página. Estos archivos del navegador se acumulan con el paso del tiempo.
Errores de programa	Durante el funcionamiento normal del equipo, algunos programas crean archivos temporales para mejorar la eficacia. Si un programa se cierra de forma inesperada debido a un error de software, es posible que estos archivos temporales queden en el disco.

4.Conceptos básicos investigación de incidentes

- Una **vulnerabilidad** es básicamente una debilidad o fallo que está presente en un sistema de información y que permite a un atacante violar la confidencialidad, integridad e incluso la disponibilidad de la información y los datos del sistema.

Principales causas de vulnerabilidades en los sistemas

Diseño	• Debilidad en el diseño de los protocolos utilizados en las redes. • Políticas de seguridad deficientes o inexistentes
Implementación	• Errores de programación • Existencia de “puertas traseras” en los sistemas • Descuido de los fabricantes
Uso	• Configuración inadecuada de los sistemas informáticos • Desconocimiento y falta de sensibilización de los usuarios y de los responsables del sistema • Disponibilidad de herramientas que facilitan los ataques de seguridad • Errores en la gestión de recursos
Vunerabilidad del día cero	• Cuando no exista una solución “conocida” para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como “vulnerabilidad 0 days”.

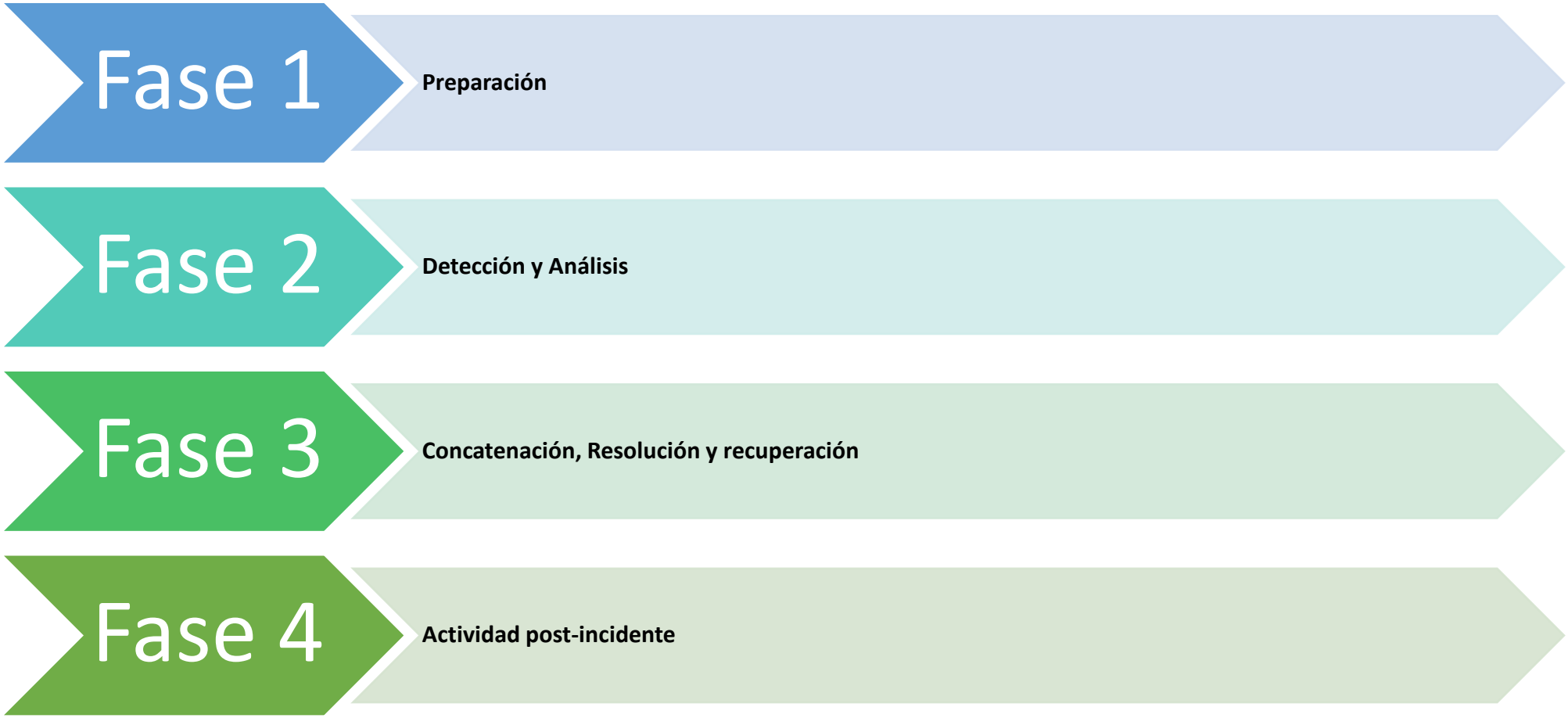
Clasificación de vulnerabilidades

Clasificación	Definición
Crítica	Permite la propagación de amenazas sin que sea necesaria la participación del usuario.
Importante	Pone en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios, como así también, la integridad o disponibilidad de los recursos de procesamiento que este disponga.
Moderada	El riesgo que presenta esta vulnerabilidad se puede disminuir con medidas tales como configuraciones predeterminadas, auditorías y de más. Estas vulnerabilidades no son aprovechables en todo su potencial ya que no afecta a una gran masa de usuarios.
Baja	Este tipo de vulnerabilidad es realmente muy difícil de aprovechar por un atacante, y su impacto es mínimo, ya que no afecta a una gran masa de usuarios.

Tipos de ataques que se aprovechan de las vulnerabilidades más conocidas

- **Desbordamiento buffer**
- **Errores de configuración**
- **Errores Web**
- **Errores de protocolo**

Gestión operativa de un incidente de seguridad



Fase 1: Preparación

NECESIDADES	OBSERVACIONES
➢ **Personal que se va a encargar de la gestión de incidentes de seguridad de la organización.**	Puede estar compuesto por un equipo o ser posiciones unipersonales
➢ **Documentación específica sobre los sistemas y redes empleados en la organización**	Permite determinar el inventario de activos de la organización
➢ **Evaluación de la actividad "normal" de la organización**	Se debe definir cuál es la actividad "normal" para poder llegar a detectar actividades sospechosas que puedan sean indicios de incidentes de seguridad.

Fase 2: Detección y análisis

- **Signos indicadores:** Estos signos ponen de manifiesto que un incidente ha ocurrido o puede estar ocurriendo:
  - Alertas de sensores que avisan de errores en el software de un servidor
  - Alerta del antivirus que informa sobre alguna infección,
  - Caída de un servidor o sistema, Accesos lentos
- **Signos precursores:** Estos signos indican la probabilidad que un incidente pueda ocurrir en el futuro:
  - La detección de un escáner de puertos de determinados sistemas de la organización para controlar cuales están disponibles
  - El resultado del análisis de vulnerabilidades
  - Las amenazas de ataque por parte de hackers

Fase 3: Contención, Resolución y Recuperación

Actividades de resolución	Actividades de recuperación
➢ **Instalación de parches de seguridad**	➢ Restaurar información desde las copias de seguridad (backups)
➢ **Cambios en las reglas cortafuegos**	➢ Reemplazar componentes afectados con otros limpios de infección
➢ **Cambios en las listas de acceso**	➢ Instalar actualizaciones de software
➢ **Cambios en los permisos de los usuarios**	➢ Modificar contraseñas
	➢ Reforzar el perímetro de red, revisando la configuración del cortafuegos

Fase 4: Actividades post-incidente

- Es muy recomendable que las organizaciones dispongan de un método de registro común para todos los incidentes de seguridad, por ejemplo un documento donde se describa, al menos:
  - Origen del incidente y persona que detecta el incidente
  - Servicio y sistemas afectados
  - Fecha/hora de inicio y cierre del incidente
  - Responsable de la gestión del incidente
  - Acciones tomadas para la resolución del mismo

Detección proactiva de incidentes de seguridad

HERRAMIENTA	CARACTERÍSTICAS
Listas maliciosas de nombres de dominio, IP y URL	Servicio que identifica nombres de dominio, direcciones IP y URL involucradas en actividades maliciosas.
Listas negras de spam	Identifica dominios, subredes y direcciones IP origen de envíos de emails de spam.
Sandbox	Entorno en el que se puede ejecutar de forma aislada un código o aplicación sospechosa sin afectar al entorno de explotación. Todo el comportamiento del software analizado es registrado y partir de esta información se determina si el software es malicioso o no.
Cortafuegos:	Dispositivo o aplicación diseñada para filtrar tráfico de red. Es recomendable filtrar tanto el tráfico saliente como el tráfico entrante.
WAF (Web application firewall):	Cortafuegos específico para aplicar reglas de filtrado sobre comunicaciones http. Generalmente son reglas que cubren ataques comunes como XSS e inyecciones SQL.
IDS/IPS:	Dispositivos hardware y/o software que monitorizan y analizan el tráfico de red o el comportamiento del sistema operativo para detectar actividades no autorizadas o maliciosas. Los IDS funcionan en modo pasivo, es decir, detectan amenazas, registran la información y disparan una alerta; sin embargo, los IPS funcionan en modo activo, lo cual les permite bloquear los comportamientos maliciosos detectados.
DLP:	Software diseñado para detectar potenciales brechas y filtraciones de datos y prevenirlos a través de monitorización, detección y bloqueo de información sensible mientras está en uso, en movimiento y en reposo. Dicha información puede ser información de propiedad intelectual, información financiera, etc.
Antivirus/Antimalware:	Software utilizado para prevenir, detectar y eliminar virus, gusanos y código malicioso de las tecnologías de información y operación. Permite cubrir puestos cliente y servidor, así como tráfico http, e-mail, etc.
SIEM (Sistema de gestión de eventos de seguridad)	Sistema que centraliza el almacenamiento y análisis de información relevante de seguridad generada por dispositivos, equipos informáticos y aplicaciones.

5.Phishing

¿Qué tipo de información roba?

- **Datos personales:**
  - Direcciones de correo
  - DNI
  - Datos de localización y contacto
  - Numero seguridad social
- **Información financiera:**
  - Números de tarjetas de crédito
  - Número de cuenta
  - Información de Home Banking o e-commerce
- **Credenciales de acceso:**
  - Redes Sociales
  - Cuentas de correo

¿Cómo se distribuye el phishing?

- Correo electrónico
- Redes Sociales
- SMS/MMS
- Llamadas telefónicas
- Infección de malware

Tipos de Phishing

- Phishing engañoso
- Spear-Phishing
- Whale-phishing
- SMS Phishing
- Voice Phising o Vishing

Recomendaciones para evitar ser víctima de phishing

- **No entregar nunca datos por correo electrónico**. Las empresas y entidades bancarias jamás solicitan datos financieros o de tarjetas de crédito por correo.
- **Ser precavido ante los correos que aparentan ser de entidades bancarias o servicios conocidos** (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.
- Se debe **sospechar si se encuentran errores gramaticales en el texto**, pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.
- Se debe estar **alerta ante comunicaciones anónimas** del tipo "Estimado cliente", "Notificación a usuario" o "Querido amigo", se trata de un posible indicio de phishing.

Recomendaciones para evitar ser víctima de phishing

- Si el mensaje obliga a tomar una decisión de **manera inminente** o en unas pocas horas, es mala señal. Se debe contrastar directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.
- Los servicios con cierto prestigio utilizarán siempre sus **propios dominios** para las direcciones de email corporativas. Si se recibe la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, se debe sospechar.
- Ante duda de la veracidad de un correo electrónico, **jamás hacer clic** en un enlace incluido en el mismo.
- Cuando se sospecha de un mensaje se debe **Ignorar** y no responder.
- Se debe comprobar que la página web en la que ha entrado es una **dirección segura**, ha de empezar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado del navegador.
- **Verificar la dirección del sitio web** que desea visitar ya que existen cientos de intentos de engaños de las páginas más populares con solo una o dos letras de diferencia.

¿Qué hacer si se detecta un phishing?

- No facilitar la información que solicitan ni contestar en ningún caso a estos mensajes. En caso de duda se debe consultar directamente a la empresa o servicio que supuestamente representan a través de sus canales oficiales.
- No acceder a los enlaces facilitados en el mensaje ni descargar ningún documento adjunto que puede contener, podría tratarse de malware.
- Eliminar el mensaje y si se puede, alertar a tus contactos sobre este fraude para que ellos no caigan tampoco en la trampa.

6.seguridad en el correo electrónico

Amenazas frecuentes asociadas al correo electrónico

- Spam
- Scam
- Cadenas de mensajes
- Phishing

lun 05/06/2017 16:38

[redacted]@[redacted]

La crisis ha acabado, Trabajen con nosotros!

Para [redacted]

¡Hola!

estamos en búsqueda de empleados que trabajen a distancia.
Mi nombre es Nuncio, soy el gerente de personal de una gran empresa internacional.

La mayor parte del trabajo usted puede realizar desde casa, es decir, a distancia.
Salario es de 2500 a 5000 EUR.

Si usted está interesado en esta oferta de trabajo, a continuación,
por favor visite **Nuestro Sitio**


Actualización de datos personales
ING
People in progress
Hola,
En ING queremos estar cerca de ti y poder ofrecerte un servicio cada día mejor.
Para ello, es necesario que actualices tus datos personales entrando en el "Área Clientes" de nuestra web y siguiendo los pasos que te detallaremos.
Área Clientes
Atentamente,
ING
IMPORTANTE: No contestes a este correo, la dirección desde la que se envía este mensaje no está habilitada para la recepción de mensajes. Recuerda que ING nunca te enviará por correo electrónico solicitud alguna para que informes de tus datos personales ni de tus claves.
protege tu empresa
PHISHING

¿Qué puede pasar si alguien accede a tu correo electrónico?

- **Perdida de privacidad**
  - Conversaciones privadas pueden quedar expuestas
  - Acceso a contactos y documentación enviada/recibida por email:
    - Facturas
    - Nóminas
    - DNI
    - Fotografías
    - Videos
- **Problemas de seguridad**
  - Perdida de acceso a la cuenta, un atacante podría cambiar la contraseña de acceso a la cuenta o modificar los métodos de recuperación de la cuenta alternativos, introduciendo otra dirección de email alternativa, otro número de teléfono, etc
  - Otro servicios asociados a la dirección de la cuenta de correo pueden verse afectados: Paypal, Facebook, Amazon, Dropbox,etc
- **Suplantación de identidad**
  - Envío de todo tipo de mensajes suplantando la identidad de un usuario para:
    - Dañar su reputación
    - Ciberacosar a otras personas
    - Enviar correos fraudulentos: malware, scam, phishing,etc
- **Poner en circulación bulos y spam.**

Consejos para un uso seguro del correo electrónico

- Contraseñas robustas
- Empleo de diferentes cuentas de correo electrónico
- Usar la opción de copia oculta (CCO o BBC)
- Desactivar el HTML en las cuentas de correo electrónico
- Cifrar el correo electrónico confidencial
- Consejos de carácter general para la seguridad del correo electrónico

Consejos para un uso seguro del correo electrónico

- Guía 821 CCN-STIC
- Robusta:
    - Longitud mínima 8 caracteres
    - Mayúsculas, minúsculas, números y símbolos
- No compartida
- No repetida
- Doble factor de autenticación
- Gestores de contraseñas

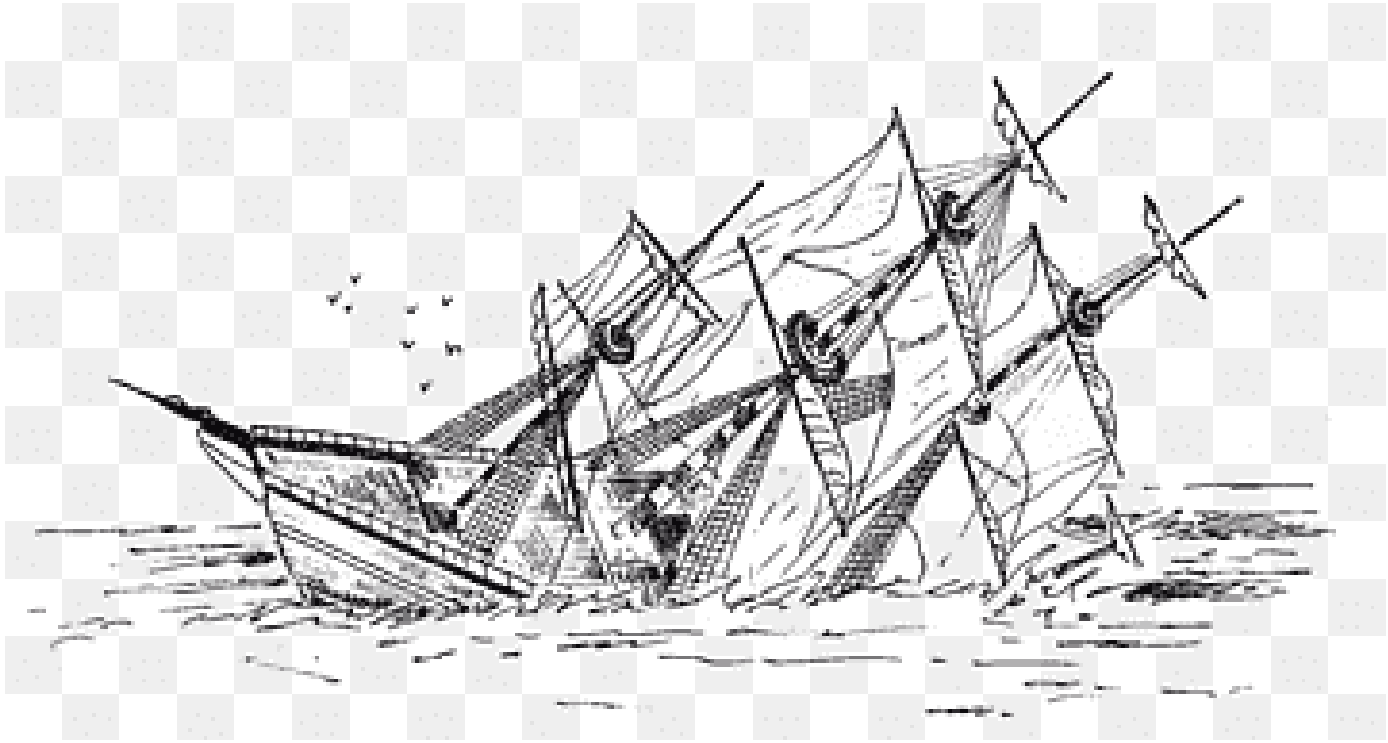
Consejos de carácter general para la seguridad del correo electrónico

- No usar de forma habitual el correo electrónico para enviar y recibir información sensible.
- Evitar acceder al correo electrónico desde equipos públicos.
- Usar con precaución las redes Wi-Fi públicas, puede haber alguien capturando las contraseñas de los usuarios.
- No ejecutar los archivos adjuntos que provengan de remitentes desconocidos.
- Evitar hacer clic en los enlaces incrustados en los correos que provienen de desconocidos o direcciones no confiables, se debe acceder siempre directamente a la web indicada, tecleando su dirección en el navegador.
- Es recomendable estar actualizado en materia de seguridad informática.
- Siempre que el servicio lo proporcione, se debe activar la verificación en dos pasos, con el fin de añadir una capa extra de seguridad en el proceso de autenticación.
- Realizar copias de seguridad para que no perder información de valor en caso de problema con el servidor de correo.
- No publicar direcciones de correo electrónico en la web de la empresa ni en sus redes sociales
- Nunca responder al correo basura

Herramientas de protección del correo electrónico

- Filtro Anti-Spam
  - Listas Negras
  - Lista blancas
- Filtros antiphishing
- Cortafuegos o firewall
- Cifrado de correos

7.Navegación segura por la red



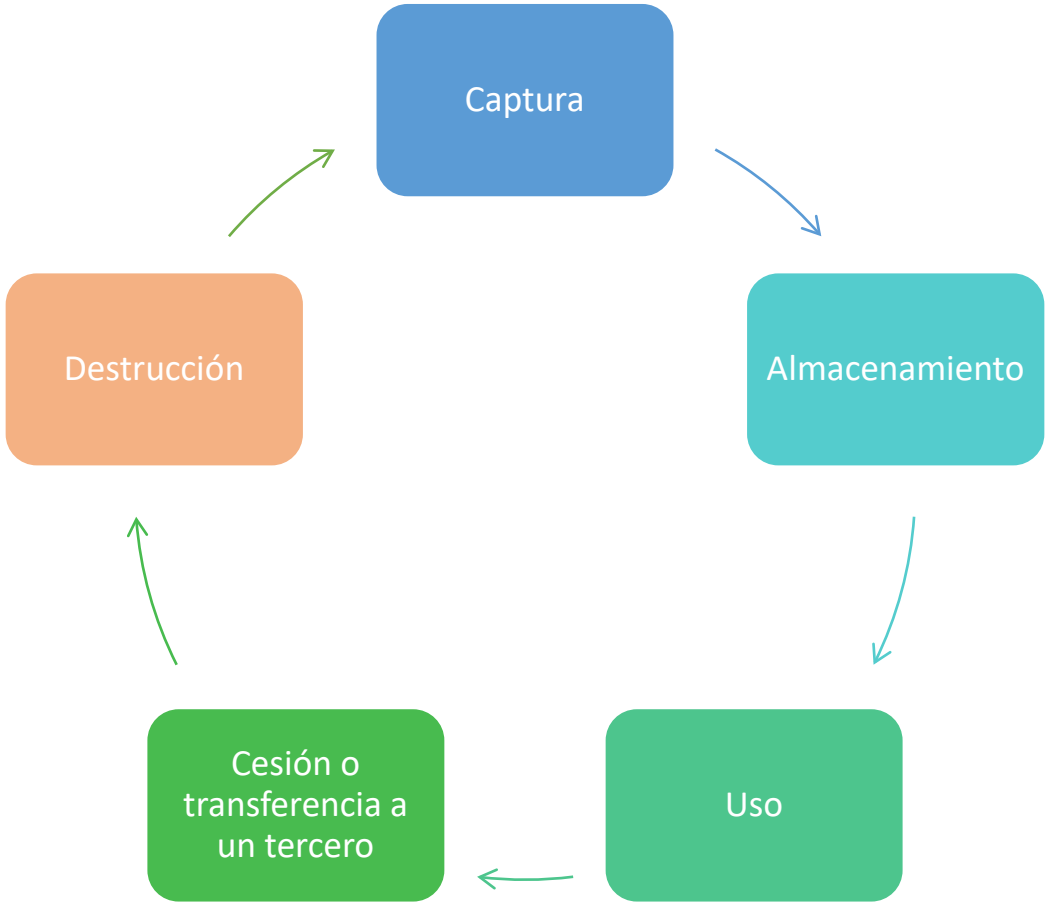
Cómo me atacan

- Introducción de código malicioso en el equipo a través de una vulnerabilidad del navegador (tenemos que visitar una página infectada)
- Manipulación e intercepción de las comunicaciones
- Descarga y ejecución de ficheros y fuentes no confiables

Aviso para navegantes

- Actualiza
- Verifica y actualiza plugins y extensiones
- Gestiona seguridad y privacidad en el navegador
- Nunca guardes contraseñas en el navegador cuando te den la opción
- Elimina las cookies de la sesión
- Modo privado
- Verifica que los sitios por los que navegas son fiables

8.Protección y destrucción de datos



Consecuencia de una incorrecta destrucción de la información

- El RGDP establece:

- *«Art. 92.4 Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.»*

- *«112.2 Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.»*

Consecuencia de una incorrecta destrucción de la información

- **Graves sanciones económicas**
- **Costes de conservación y custodia**
- **Daños de imagen**
- **Seguridad**

Métodos seguros de destrucción de documentación electrónica

- Factores a tener en cuenta a la hora de destruir información

- Se almacena en soportes de almacenamiento con un formato específico
- Los soportes son generalmente reutilizables
- Su vida útil es corta comparada con la de un soporte en papel
- Todo soporte o formato se hará obsoleto en un plazo más o menos largo de tiempo, lo que implicará necesariamente un cambio de soporte o formato (excepto algunos formatos longevos como PDF/A).
- Los procedimientos de destrucción deberán tener en cuenta las características de los soportes más adecuados para la conservación de los documentos electrónicos.

- Pueden existir múltiples copias, no siempre controladas, de los documentos

Sobreescritura total

- *elimina la información sin que ésta pueda ser recuperada y permite volver a utilizar el dispositivo con garantías de que funcione correctamente*
- *se utiliza habitualmente con todos los dispositivos regrabables (discos duros, USB, etc), también se suele usar en la reutilización de dispositivos como: equipos de sobremesa o equipos portátiles para tener la seguridad de que toda la información eliminada es irrecuperable*
- *La sobreescritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados*
- *Este método de destrucción segura de la información es el que dispone del mayor número de ventajas*
  - Se puede utilizar para todos los dispositivos regrabables.
  - Tras el proceso de borrado es posible acceder de nuevo al dispositivo para certificar que todos los datos que se encontraban almacenados previamente han sido sustituidos por el patrón de borrado.
  - Es posible realizar la operación de borrado en las propias oficinas de la empresa, evitando el transporte a un centro de reciclaje autorizado.
  - Permite la reutilización de los dispositivos.

Desmagnetización

- *La desmagnetización es un proceso de borrado seguro, que consiste en la exposición de los soportes de almacenamiento de información a un potente campo magnético proporcionado por un equipo electrónico desmagnetizador, este proceso permite eliminación permanente de los datos almacenados en el dispositivo*
- Antes de emplear este método es importante conocer los inconvenientes que presenta el proceso de desmagnetización:
  - Los dispositivos deben trasladarse al lugar donde se encuentre el desmagnetizador, lo que implica unos costes de transporte y el aseguramiento de la cadena de custodia
  - Los dispositivos dejan de funcionar correctamente tras ser sometidos al proceso y por tanto requieren de un reciclado que sea respetuoso con el medio ambiente.
  - La comprobación de que todos los datos han sido borrados completamente es prácticamente imposible, ya que al dejar de funcionar los dispositivos no es posible acceder a ellos para certificar el borrado.
  - Se debe analizar el dispositivo que se desea borrar y aplicar el campo magnético necesario. En ocasiones se opta por aplicar la máxima potencia, desperdiciando energía de forma innecesaria.

Destrucción física

El objetivo de la destrucción física es la inutilización del soporte que almacena la información para evitar la recuperación posterior de los datos que almacena.

Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento:

- **Desintegración:** mecanismo de corte o triturado no uniforme que reduce el dispositivo a pedazos de tamaño y forma aleatorios.
- **Pulverización:** proceso que consiste en machacar el material y que se utiliza para la destrucción de discos duros.
- **Fusión:** proceso mediante el cual el material se calienta a una temperatura que es menor que el punto de encendido pero suficientemente alta para derretirlo, puede ser un medio efectivo de destrucción para los discos duros
- **incineración:** puede destruir completamente todos los dispositivos y para todos los niveles de seguridad. Debe llevarse a cabo en incineradoras que hayan sido aprobadas en cuanto a impacto medioambiental, para plásticos y otros materiales.
- **Trituración:** consiste en reducir el soporte a pedazos minúsculos de tamaño y forma uniformes. El uso de trituradoras está normalmente limitado a soportes de grosor fino, como los soportes de datos ópticos (DVDs o CDs).

Inconvenientes métodos de destrucción física

- Los **residuos generados**, que deben ser tratados adecuadamente
- La utilización de **distintos métodos** industriales de destrucción según el tipo de soporte
- En muchas ocasiones obligan a un **transporte** de los dispositivos a un centro de reciclaje adecuado
- La **certificación de la destrucción** en compleja, ya que no es posible acceder a los dispositivos para confirmar que la información ha sido eliminada y se deben hacer comprobaciones manuales, como fotografías y anotación de número de serie que certifique que el dispositivo ha sido eliminado.

Comparativa

Método de borrado	Ventajas	Inconvenientes	Soportes sobre los que se pueden aplicar
Sobrescritura	• Eliminación de forma segura de la información	• No válido para dispositivos no regrabables	Discos Duros (magnético)
	• Solución única para todos los dispositivos	• No válido para dispositivos ópticos	Cintas de Backup (magnético)
	• Certificación de la operación		USBs (electrónico)
	• Posibilidad de eliminación en la propia oficina		Discos Duros SSD (electrónico)
	• Reutilización de los dispositivos con garantías de funcionamiento		
Desmagnetización	• Eliminación de forma segura de la información	• Una configuración del sistema para cada soporte	Discos Duros (magnético)
		• Dificultad de certificación del proceso	Cintas de Backup (magnético)
		• Transportar los equipos a una ubicación externa	
		• Sólo válido para dispositivos magnéticos	
		• Inutilización final del dispositivo	
Destrucción física	• Eliminación de forma segura de la información	• Un sistema de destrucción para cada soporte	Discos Duros (magnético)
	• Destrucción de dispositivos no regrabables	• Dificultad de certificación del proceso	Cintas de Backup (magnético)
	• Destrucción de dispositivos ópticos	• Transportar los equipos a una ubicación externa	CD (óptico)
		• Inutilización final del dispositivo	DVD (óptico)
		• Dificultad de reciclaje de materiales	USBs (electrónico)
			Discos Duros SSD (electrónico)

Contratación de una empresa externa para la destrucción de documentos

Una opción aconsejable, tanto para empresas como para organizaciones, cuando el volumen de la documentación es elevado o no se dispone de los medios técnicos exigidos para su destrucción, es la contratación de una empresa externa especializada

- Se debe establecer un contrato por escrito con la empresa contratada, en el que se regulen todas las transacciones.
- Se debe exigir la entrega de los certificados correspondientes de destrucción.
- Se debe exigir que un representante del responsable de los documentos presencie la destrucción de los documentos y compruebe las condiciones en que se realiza y los resultados.
- Se debe garantizar la destrucción de los documentos en sus instalaciones y con medios propios, sin subcontratos que conlleven el manejo de los documentos por parte de otras empresas sin conocimiento del responsable de los documentos.
- La destrucción debe realizarse al nivel adecuado conforme a la confidencialidad de los documentos y del material que se tiene que destruir.
- El personal que lleva a cabo la recogida, transporte y destrucción debe contar con la formación adecuada, así como suscribir un compromiso de confidencialidad.
- Se debe exigir que cumplan con la legislación que les aplica por su actividad, por el tratamiento de los datos que realizan y por el potencial impacto medioambiental.

Políticas de borrado seguro

Toda empresa u organización debe disponer de una “Política de Borrado Seguro de la información”. Dicha política debe contener:

- **Una gestión de soportes adecuada:**
  - Se debe realizar un seguimiento de todos los dispositivos que están en funcionamiento, así como de las personas o departamentos responsables de cada uno, de la información contenida en ellos y de su clasificación en función del grado de criticidad para el negocio.
  - Se debe llevar a cabo la supervisión de los dispositivos que almacenan las copias de seguridad de esos datos.
  - Se debe controlar cualquier operación realizada sobre un dispositivo: mantenimiento, reparación, sustitución, entre otros.
  - Además en los traslados de los dispositivos de almacenamiento a instalaciones externas a las de la empresa para su borrado/destrucción, se debe asegurar que se cumple la cadena de custodia de los mismos, para evitar fugas de información.

- **La documentación de las operaciones de borrado realizadas:**
  - Se debe elegir aquellas herramientas de borrado que permitan obtener un documento que certifique que el proceso de borrado ha sido realizado correctamente, además dicho documento debe especificar cuándo y cómo ha sido realizado.
  - En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, este hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosa con el medio ambiente.

9.Redes sociales

Uso malicioso de redes sociales

- Ingeniería social
- Robo de identidad
- Ciberacoso
  - **Ciberbullying**
  - **Grooming**
  - **Sextorsión**
  - **Sexting**
- *Los contenidos publicados por los usuarios en las distintas redes sociales puedes acarrear un perjuicio en su **reputación** que puede afectar en el ámbito personal, social o laboral.*
- Publicidad dañina o engañosa
- Delitos físicos (robos)
- Distribución de malware

Publicaciones en redes sociales

Tipos de datos personales poseen las redes sociales

- **Datos del contenido compartido** textos, fotos, vídeos, actualizaciones de estado,
- **Datos intrínsecos de las fotos subidas**: dispositivo desde el que se realiza la foto, fecha, hora, lugar, calidad, formato, ubicación
- **Mensajes enviados**
- **Lista de contactos**
- **Datos del perfil**
- **Datos de interacciones**
- **Localización**

Como usan las redes sociales estos datos

- **Para sugerir información**
- **Para crear perfiles de usuario**
- **Para vender a terceros**
- **Definir patrones de comportamiento**
- **Para generar emoción**

tipo de información no se debe publicar

Fecha de nacimiento completa	• Suele ser necesaria a la hora de crear un perfil en una red social, sin embargo, puede no ser visible para los contactos, ya que trata una pieza clave para los robos de identidad o para extorsiones.
Nombre completo o DNI	• Se trata de información muy valiosa para los atacantes, sobre todo para la suplantación de identidad.
Ubicación actual	• Publicar la ubicación puede ser muy peligroso, ya que se está informando de cuando una casa deshabitada o informar acerca de las rutinas diarias de un usuario, como, por ejemplo, el tiempo que pasa en el trabajo o en el gimnasio.
Domicilio	• Dejar el domicilio a la vista de todos puede facilitar el robo de una vivienda o la suplantación de identidad.
Número de móvil o correo electrónico	• Este tipo de datosaporta mucha información a terceras personas que busquen realizar algún tipo de ataque por medio de ingeniería social.

	Buenas prácticas en el uso de redes sociales
1	Reflexionar sobre los contenidos publicados en las redes sociales
2	No compartir información sensible ya sea propia o ajena: documentos identificativos, números de teléfono, direcciones postales, localizaciones exactas, identificadores de vehículos, etc.
3	No hacer clic en contenidos de los que no se tenga claro su origen o contenido
4	Tener caudado con los mensajes de desconocidos
5	No compartir fotos ni vídeos en situaciones comprometidas
6	Desactivar la geolocalización por defecto y hacer un uso inteligente de la misma.
7	Comprobar la configuración de seguridad tanto en el perfil de usuario como en los contenidos que se comparten
8	No difundir información privada sobre otras personas sin su consentimiento y no etiquetar por su nombre a otras personas que no tienen perfil en redes sociales sin solicitar previamente su permiso para hacerlo.
9	Mantener en privado la lista de contactos y analizar en detenimiento las solicitudes de amistad de desconocidos.
10	Cerrar aquellas cuentas que no se estén usando
11	Verificar que apps están conectadas a las redes sociales
12	Utilizar un correo electrónico único para el uso de las redes sociales
13	Mantener las aplicaciones móviles actualizadas
14	Proteger el acceso a los perfiles en redes sociales con contraseñas fuertes utilizando dos factores de autenticación donde sea viable.
15	Configurar adecuadamente la privacidad del perfil de usuario
16	Ante cualquier problema de seguridad, contactar con la red social.
17	Leer la política de privacidad y las condiciones del servicio antes de usarlo
18	Vigila los permisos otorgados a los juegos o aplicaciones y evitar aquellas que requieren autorizaciones que no son necesarias como: acceso al correo electrónico, fotografías, información de nuestros contactos, etc.
19	No publicar contenido ni realizar ninguna acción que viole la ley o infrinja los derechos de propiedad intelectual del Grupo o de terceros.
20	Contrasta la información leída en las redes sociales, podría ser falsa o publicidad engañosa.

10.Reglamento General de Protección de Datos

*El **Reglamento General de Protección de Datos**, constituye un nuevo marco jurídico sobre la protección de los datos personales y sobre sobre su libre circulación.*

Se trata de la primera norma sobre la protección de datos de carácter personal que afecta a todos los países de la Unión Europea y unifica, por tanto, tanto los derechos como las obligaciones

Está diseñado para otorgar mayor seguridad y control a las personas sobre su información personal, así como para establecer unas reglas comunes en toda Europa para la protección de dicha información

Ámbito subjetivo y objetivo del RGPD

- Subjetivo
  - empresas o entidades que traten datos personales como parte de las actividades de una de sus sucursales establecidas en la Unión Europea (UE), independientemente del lugar donde sean tratados los datos.
  - En empresas establecidas fuera de la Unión Europea que ofrecen productos o servicios, ya sea de pago o gratuitos, o realizan observaciones del comportamiento de las personas en la Unión Europea.
- Objetivo
  - Cualquier tratamiento total o parcialmente automatizado de datos personales.
  - Tratamientos no automatizados de datos personales contenidos o destinados a ser incluidos en un fichero.
- El RGPD no se aplica a tratamientos de datos personales:
  - Efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticos.
  - Efectuados por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.
  - De personas fallecidas.
  - Destinados a la seguridad Nacional.

Incumplimiento y sanciones del RGPD

- **artículo 82.1** "*toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos*“

- **artículo 83.5** *referencia a la cuantía de las multas administrativas, de manera que dependiendo del artículo del RGPD que haya sido vulnerado, las multas impuestas pueden ir desde los 10 millones de euros (o el 2 % como máximo del volumen de negocio total anual global) hasta los 20 millones de euros (o el 4 % como máximo del volumen de negocio total anual global).*

- demás de las sanciones económicas, el nuevo RGPD prevé tres medidas adicionales o apercibimientos, de menor a mayor importancia:
  - Advertencia
  - Amonestación
  - Suspensión del tratamiento de datos

Conceptos básicos del RGPD

- Datos personales
- Tratamiento de datos de carácter personal
- Responsable del tratamiento
- Encargado del tratamiento
- Autoridad de Protección de Datos
- Delegado de protección de datos
- Responsabilidad proactiva
- Consentimiento del interesado

Datos especialmente protegidos

Datos de Salud

- Relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Datos Genéticos

- Relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Datos Biométricos

- Relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

¿Qué derechos tiene un ciudadano?

1. Derecho de acceso
2. Derecho de rectificación
3. Derecho de oposición
4. Derecho de Supresión
5. Dereho de limitación del tratamiento
6. Derecho de portabilidad
7. Derecho de oposición al tratamiento automático

Características de los derechos

- Su ejercicio **gratuito**
- Si las solicitudes son **manifiestamente infundadas** o excesivas (p. ej., carácter repetitivo) el responsable podrá:
  - Cobrar un canon proporcional a los costes administrativos soportados
  - Negarse a actuar
- Las solicitudes deben responderse en el **plazo de un mes**, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más
- El responsable está **obligado a informarte** sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio
- Si la solicitud se presenta por **medios electrónicos**, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo
- Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las **razones de su no actuación** y la posibilidad de reclamar ante una Autoridad de Control
- Puedes ejercer los derechos directamente o por medio de tu **representante legal** o voluntario
- Cabe la posibilidad de que el **encargado** sea quien atienda tu solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule

11.Seguridad en los dispositivos moviles

Riesgos más habituales

- Pérdida, robo o destrucción de dispositivos
- Robo de credenciales
- Dispositivos poco seguros
- Aplicaciones peligrosas
- Conexiones a redes inseguras
- Geoposicionamiento
- Hábitos de usuario peligrosos

Medidas de seguridad

Tanto los dispositivos móviles personales para uso profesional como la información corporativa que manejan, deben estar protegidos convenientemente, estableciendo unas adecuadas medidas de seguridad que ayuden a minimizar todo lo posible los riesgos a los que están expuestos

- Aplicaciones instaladas
  - Descargar e instalar únicamente aplicaciones permitidas en las políticas de seguridad de la empresa.
  - Leernos siempre las condiciones de uso e instalación de cada aplicación, de modo, que se puedan controlar los permisos de acceso sobre los dispositivos móviles.
  - Descargar las aplicaciones siempre de sitios oficiales para evitar la instalación de malware.
- Almacenamiento en la nube
  - Tener en cuenta la disponibilidad de los datos en el caso de que el servicio de nube este en mantenimiento, fuera de servicio o sufra algún tipo de incidente de seguridad**.**
  - Conocer las restricciones del proveedor con respecto al tipo de datos que se pueden almacenar en la nube.
  - Saber el tipo y la frecuencia con las que el servidor realiza las copias de seguridad de sus servidores
  - Configurar los dispositivos móviles de modo que no mantengan habilitado el acceso directo a los datos, sino que obligue a los usuarios a introducir siempre la contraseña, cada vez que se acceda al servicio.

- Copias de seguridad
  - Almacenar las copias de seguridad fuera de los dispositivos móviles, ya sea en servidores propios de la empresa u organización o en servicios de nube
  - aplicarse las medidas necesarias para proteger la privacidad de esos datos personales.
  - Las copias de seguridad deberían realizarse de manera automática cada cierto tiempo.
- Cifrado
  - es recomendable cifrar la información almacenada en los dispositivos móviles, reduciendo así el impacto que podría ocasionar la pérdida o robo de un dispositivo móvil.
- Localización remota. Se deben aplicar los siguientes parámetros
  - Localización del dispositivo
  - Bloqueo remoto del terminal
  - Borrado remoto de datos
  - Seguimiento de actividad del dispositivo
- Configuración de los dispositivos
  - Habilitar sistemas de autenticación robustos de acceso al sistema.
  - Configurar la realización automática de copias de seguridad periódicas
  - Configurar la actualización automática de software
  - Instalar y configurar un antivirus
  - Desactivar el permiso de recuerdo de contraseña
  - Habilitar la funcionalidad que permita restablecer la configuración por defecto del dispositivo vía remota
  - Habilitar los mecanismos de bloqueo automático del dispositivo

- Geolocalización
  - Deshabilitar esta funcionalidad siempre que su uso no sea estrictamente necesario
  - Ser consciente de que la utilización de este servicio puede implicar la violación de la privacidad de los empleados, por ello, se debe informar a los empleados y firmar acuerdos de consentimiento

- Conexiones a redes Wifi públicas
  - Desconfiar de las redes wifi públicas o gratuitas
  - Utilizar redes virtuales privadas (VPN) como canal de comunicación o algún otro tipo de cifrado punto a punto, como los sitios web con protocolo SSL y certificados digitales
  - Desconectar la función wifi de los dispositivos móviles cuando no se esté utilizando
  - Deshabilitar la conexión automáticas a redes
  - Preferentemente hacer uso de las redes 3G o 4G antes que de redes wifi inseguras
- Concienciación y formación de los usuarios. un empleado concienciado:
  - Comprenderá y cumplirá las normas y políticas de seguridad establecidas por la organización para el uso los dispositivos móviles
  - Sabrá gestionar los posibles incidentes de seguridad relacionados con los dispositivos móviles
  - Evitará la realización de acciones indeseadas sobre la información y los dispositivos móviles

12.Deberes y obligaciones del empleado

	Normas generales de uso de equipos
	1. Únicamente podrán emplearse para fines institucionales 2. Sólo el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos 3. Está prohibido alterar, cualquiera de los componentes físicos o lógicos de los equipos 4. No se tendrán privilegios de administración sobre los equipos 5. Se facilitará, al personal de soporte técnico, el acceso a los equipos para labores de reparación, instalación o mantenimiento 6. Comunicar cualquier comportamiento anómalo en los equipos 7. Se debe participar en el cuidado y mantenimiento del equipo 8. Hacer un uso responsable de dispositivos como: USC, DVDs,CDs 9. No está autorizado el uso de memorias USB, salvo autorización expresa 10. El uso de equipos grabadores de CDs y DVDs no está autorizado. 11. No se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por la organización 12. Antes de abandonar las salas o permitir que alguien ajeno entre, se deben limpiar adecuadamente las pizarras y flipcharts de las salas de reuniones o despachos 13. Se debe apagar el pc al finalizar la jornada laboral.

	Usos especialmente prohibidos en equipos
	1. Ejecución remota de archivos de tipo audiovisual 2. Utilización de cualquier tipo de software dañino 3. Utilización de programas que hagan un uso abusivo de la red 4. Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la organización 5. Utilización de conexiones y medios inalámbricos con tecnologías Wifi, Bluetooth o infrarrojos que no estén debidamente autorizados 6. Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet 7. Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual 8. Está totalmente prohibido toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas

Normas para el almacenamiento de información

1. No se almacenará información en los ordenadores de forma local
2. Almacenar únicamente la información estrictamente necesaria en las unidades de red compartidas
3. No está permitido almacenar información privada, en los recursos de almacenamiento compartidos o locales
4. Se debe guardar bajo llave, aquella información impresa que sea necesario almacenar

Normas impresoras, fotocopiadoras y faxes

1. Únicamente podrán utilizarse impresoras en red o fotocopiadoras corporativas.
2. La documentación impresa deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras.
3. Conviene no olvidar tomar los originales del escáner o de la fotocopiadora.
4. Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo
5. Cuando se digitalicen documentos se deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida
6. La documentación impresa que ya no es necesaria, deberá ser eliminada en las máquinas destructoras.
7. Por razones ecológicas y de seguridad, antes de imprimir documentos, se debe asegurar de que es absolutamente necesario hacerlo.

Normas para equipos portátiles y móviles
1. Cada equipo está bajo custodia del usuario asignado 2. Se deben adoptar las medidas necesarias para evitar daños o sustracción, así como el 3. acceso a ellos por parte de personas no autorizadas. 4. Comunicar inmediatamente incidencias por sustracción 5. Se deben emplear únicamente con fines institucionales 6. No deberán conectarse directamente a redes externas (incluyendo la red a internet del domicilio) 7. Se deberán realizar conexiones periódicas a la red corporativa 8. Cuando la información tratada así lo requiera, los ordenadores portátiles deberán: - Tener cifrado el disco duro - Disponer de software que garantice un arranque seguro - Mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema a través cualquier medio 9. Se configurarán con todos los canales, puertos y sistemas de comunicaciones de salida bloqueados (wifi, bluetooh, USB's, cd, dvd, tarjetas de red, etc.) 10. No se tendrán privilegios de administración sobre los equipos

Normas de acceso a internet

1. Usar Internet solo para fines profesionales
2. No visitar páginas de contenido poco ético, ofensivo o ilegal
3. No visitar páginas no fiables o sospechosas
4. Cuidar la información que se publica en Internet
5. Antes de utilizar una información obtenida de Internet, se debe comprobar en qué medida se halla sujeta a los derechos derivados de la Propiedad Intelectual o Industrial.
6. Realizar descargas sólo si se tiene autorización
7. No descargar código o programas no confiables
8. Asegurar la autenticidad de la página visitada
9. Comprobar la seguridad de la conexión (HTTPS)
10. Cerrar las sesiones al terminar la conexión
11. Utilizar el niveles de seguridad “alto” del navegador
12. Desactivar las cookies
13. Eliminar la información privada del navegador
14. No instalar complementos desconocido
15. Desactivar las características de recordar contraseñas en el navegador
16. Los navegadores utilizados para el acceso vía web deben estar permanentemente actualizados a su última versión
17. Activar la opción de borrado automático al cierre del navegador

Normas para el teletrabajo
1. Emplear los dispositivos móviles facilitados para trabajar fuera de las instalaciones, únicamente con fines institucionales. 2. Necesidad de autorización para el uso de documentos, equipos y dispositivos fuera de la organización 3. Necesidad de autorización para el empleo de dispositivos personales en el tratamiento de información corporativa 4. Copias periódicas de seguridad de la información contenida en dispositivos móviles 5. Uso de los canales de comunicación establecidos 6. Vigilancia permanente 7. Transporte seguro tanto de documentos como de equipos portátiles 8. Utilización de candados y/o cables de seguridad para los dispositivos móviles 9. Revisión periódica de los equipos 10. No desactivar las herramientas de seguridad habilitadas en los dispositivos móviles 11. No descargar ni instalar contenidos no autorizados en los equipos 12. Comunicar cualquier incidente con la mayor rapidez que sea posible

13.Detección y reacción ante incidentes de seguridad

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información. Se trata de un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o de incluso de una violación a la Política de Seguridad de la Información de una organización

Todo usuario del sistema debe notificar cualquier incidente de seguridad que detecte al Responsable de Seguridad de la organización. Es preferible comunicar mediante correo electrónico, que de forma presencial o telefónica

Clasificación incidentes de seguridad

CLASIFICACIÓN	TIPO DE INCIDENTE	PELIGROSIDAD
Contenido abusivo	Spam	BAJO
	Delito de odio	MEDIO
	Pornografía infantil, contenido sexual o violento inadecuado	ALTO
Contenido dañino	Sistema infectado	ALTO
	Servidor C&C	ALTO
	Distribución de malware	MUY ALTO
	Configuración de malware	MUY ALTO
	Malware dominio DGA	ALTO
Obtención de información	Escaneo de redes	BAJO
	Análisis de paquetes	BAJO
	Ingeniería social	MEDIO
Intento de intrusión	Explotación de vulnerabilidades conocidas	MEDIO
	Intento de acceso con vulneración de credenciales	MEDIO
	Ataque desconocido	MUY ALTO
Intrusión	Compromiso de cuenta con privilegios	MEDIO
	Compromiso de cuenta sin privilegios	BAJO
	Compromiso de aplicaciones	ALTO
	Robo	MUY ALTO

Disponibilidad¤	DoS·(Denegación·de·servicio)¤	ALTO¤
	DDoS·(Denegación·distribuida·de·servicio)¤	ALTO¤
Compromiso·de·la·información¤	Sabotaje¤	MUY·ALTO¤
	Interrupciones¤	MUY·ALTO¤
	Acceso·no·autorizado·a·información¤	ALTO¤
	Modificación·no·autorizada·de·información¤	ALTO¤
	Pérdida·de·datos¤	ALTO¤
Fraude¤	Uso·no·autorizado·de·recursos¤	MEDIO¤
	Derechos·de·autor¤	MEDIO¤
	Suplantación¤	MEDIO¤
	Phishing¤	MEDIO¤

Vulnerable¤	Criptografía·débil¤	MEDIO¤
	Amplificador·DDoS¤	MEDIO¤
	Servicios·con·acceso·potencial·no·deseado¤	MEDIO¤
	Revelación·de·información¤	MEDIO¤
	Sistema·vulnerable¤	MEDIO¤
Otros¤	APT¤	CRÍTICO¤
	Ciberterrorismo¤	CRÍTICO¤
	Daños·informáticos·PIC¤	CRÍTICO¤
	Otros¤	CRÍTICO¤

Impacto de cada incidente

- Los criterios empleados para la determinación del nivel de impacto asociado a un incidente atienden a los siguientes parámetros:
  - Impacto en la Seguridad Nacional o en la Seguridad Ciudadana
  - Efectos en la prestación de un servicio esencial o en una infraestructura crítica.
  - Tipología de la información o sistemas afectados.
  - Grado de afectación a las instalaciones de la organización.
  - Posible interrupción en la prestación del servicio normal de la organización.
  - Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
  - Pérdidas económicas.
  - Extensión geográfica afectada.
  - Daños reputacionales asociados.

Registro de incidentes de seguridad

- Qué información registrar
  - Clasificación del incidente
  - Fecha y hora de la detección del incidente.
  - Fecha y hora de la notificación.
  - Persona que recibe la notificación.
  - Estado: Abierta, cerrada, pendiente de confirmar, etc…
  - Dimensiones de seguridad afectadas: Confidencialidad, Disponibilidad e Integridad (si las dimensiones trazabilidad y autenticidad se ven afectadas, se considerará como un caso en que se encuentra afectada la integridad de la información).
  - Fecha y hora de la resolución y cierre.
  - Acciones llevadas a cabo para solucionarla
  - Los efectos que se hubieran derivado de la misma.
  - Proceso de recuperación (si aplica)

Que hacer con las evidencias

- Debe mantenerse un registro detallado de todas las evidencias, incluyendo:
  - La identificación de la información (por ejemplo, la localización, el número de serie, número de modelo, el nombre de host, dirección MAC y direcciones IP de los ordenadores afectados).
  - Nombre, cargo y el teléfono de cada persona que ha recogido o gestionado evidencias durante la investigación del incidente.
  - Fecha y hora de cada ocasión en la que ha sido tratada cada evidencia.
  - Ubicaciones donde se custodiaron las evidencias.

Notificación de incidentes a autoridades de control

- Comunicación de incidentes al CCN

Todos aquellos incidentes categorizados con un Nivel de Peligrosidad o impacto Alto, Muy Alto o Crítico, deben ser notificados al Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT).

Para ello, enviará un correo electrónico a la dirección incidentes@ccn-cert.cni.es indicando:

- Descripción lo más detallada posible del incidente.
- La información de contacto (al menos una dirección de correo y un teléfono).

El correo electrónico debe enviarse cifrado utilizando las claves PGP/GPG disponibles en https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html.

Notificación de incidentes a autoridades de control

- Para la resolución de incidentes y problemas de la **Red SARA**, se establecerán las comunicaciones a través del Centro de Soporte 24x7 de la Red SARA, que está activo 365 días al año.

- La organización dispondrá en todo momento de los canales de contacto y sistemática de comunicación según el tipo de incidencia a través de la propia Web:

- https://www.redsara.es/infoSARA/elements/recursos/incidencias/

Notificación de incidentes a autoridades de control

- Cuando se produzca un incidente, “brecha”, de seguridad que suponga una violación de la seguridad de los datos personales, será necesario considerar dos tipos de comunicaciones:

- **Comunicación a la Agencia Española de Protección de Datos (AEPD)**

- La comunicación a la AEPD será responsabilidad del Delegado de Protección de datos o, en su caso, del Responsable del tratamiento, la brecha deberá ser notificada lo antes posible y a más tardar 72h después de que se haya tenido constancia de ella.

- Cuando la notificación inicial no sea posible en el plazo de 72 horas, la notificación se realizará igualmente, y en ella deberán constar y justificarse los motivos de la dilación.

- La notificación a la AEPD se realizará a través del formulario destinado a tal efecto publicado en la sede electrónica de la agencia, en https://sedeagpd.gob.es/sede-electronica-web/

- Se deben cumplimentar todos datos identificativos y de contacto de la organización, Delegado de Protección de Datos, Responsable del tratamiento, información sobre la brecha de seguridad de datos personales…

- **Comunicación a los interesados afectados**

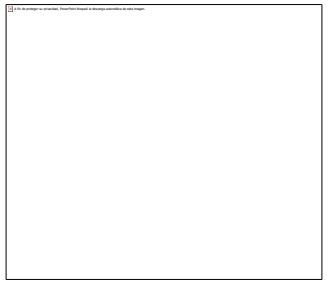
- Por otro lado, cuando sea probable que la incidencia de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el DPD (Delegado de Protección de Datos) y, en su caso, el Responsable de Tratamiento, la comunicará a los afectados mediante el procedimiento establecido por la AEPD sin dilación alguna, procurando mantener igualmente el plazo máximo de 72 horas ahora con los afectados o siempre que lo determine el DPD.

- Esta comunicación, debería contener como mínimo:

- Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
- Descripción general del incidente y momento en que se ha producido.
- Las posibles consecuencias de la brecha de la seguridad de los datos personales.
- Descripción de los datos e información personal afectados.
- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.

- Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.unicación de brechas de seguridad

Gracias por su atención!!



- **Jose Manuel Sáenz de Santa María Fernandez– VPS CONSULTING S.L.U.**
- **Mail: jose.saenz@vps-strategic.com**