TEMA 8: SEGURIDAD DE DATOS DE LA INFORMACIÓN

Presentación

Francisco Javier Mollá Alonso.

- **Director Departamento de Modernización y Nuevas Tecnologías del Ayuntamiento de Picanya**
- **Email: jmolla@picanya.org**

“La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal familiar de los ciudadanos en pleno ejercicio de sus derechos”

LEYES Y REGLAMENTOS

- LOPD 15/1999
- RGPD 2016/679
- LOPD-GDD 3/2018

SEGURIDAD DE DATOS

PALABRAS CLAVE

- DATOS
- MEDIDAS
- PROTEGER
- ACCESO
- AUTORIZADOS
- NO

¿QUÉ ES LA SEGURIDAD DE DATOS?

- Son las medidas de protección empleadas para proteger los datos contra accesos no autorizados

PRINCIPIOS DE LA SEGURIDAD DE DATOS

- LA CONFIDENCIALIDAD
- LA INTEGRIDAD
- LA DISPONIBILIDAD

PRINCIPIOS DE LA SEGURIDAD DE DATOS

LA CONFIDENCIALIDAD

- ¿Qué es un dato confidencial?
  - Es el que contiene información sensible o privada que deben protegerse de accesos no autorizado.

- MEDIDAS de PROTECCIÓN
  - Medidas técnicas
  - Medidas organizativas

PRINCIPIOS DE LA SEGURIDAD DE DATOS

MEDIDAS PARA CONFIDENCIALIDAD

¿Qué tipo de medida es?

- ACCESO RESTRINGIDO ¿es T / es O?
- ENCRIPTACIÓN ¿es T / es O?
- FIREWALLS Y SEGURIDAD DE RED ¿es T / es O?
- POLITICAS DE GRUPO GPO ¿es T / es O?
- POLITICAS DE SEGURIDAD ¿es T / es O?
- AUDITORIAS ¿es T / es O?

- Mas ejemplos ¿???

PRINCIPIOS DE LA SEGURIDAD DE DATOS

LA INTEGRIDAD

• Es un proceso para garantizar que los datos sean precisos, completos y coherentes.

•¿Es importante? ……

•¿Qué conseguimos con la integridad?.....

PRINCIPIOS DE LA SEGURIDAD DE DATOS

DISPONIBILIDAD

• Es al hecho de que los datos sean accesibles y su utilización sea para fines previstos.

•Estrategias para mejorar la disponibilidad:

- Redundancia
- Balanceo de carga
- Respaldos regulares
- Monitoreo constante
- Planificación de capacidad
- HA
- Georredundancia

LA DISPONIBILIDAD NO SE TRATA SOLO DE TECNOLOGIA SINO TAMBIÉN DE PROCESOS, CAPACITACIÓN Y PLANIFICACIÓN.

AMENAZAS DE LA SEGURIDAD DE DATOS

SEGURIDAD DE LA INFORMACIÓN

• INFOSEC: Conjunto de herramientas y procedimientos con los que proteger la información ante utilizaciones indebidas, accesos sin autorización, interrupciones de servicios, robo, destrucciones de datos.

•¿Qué engloba la seguridad de la información?

- Seguridad física y del entorno
- La ciberseguridad
- Control de acceso a la información

AMENAZAS DE LA SEGURIDAD DE DATOS

SEGURIDAD DE LA INFORMACIÓN

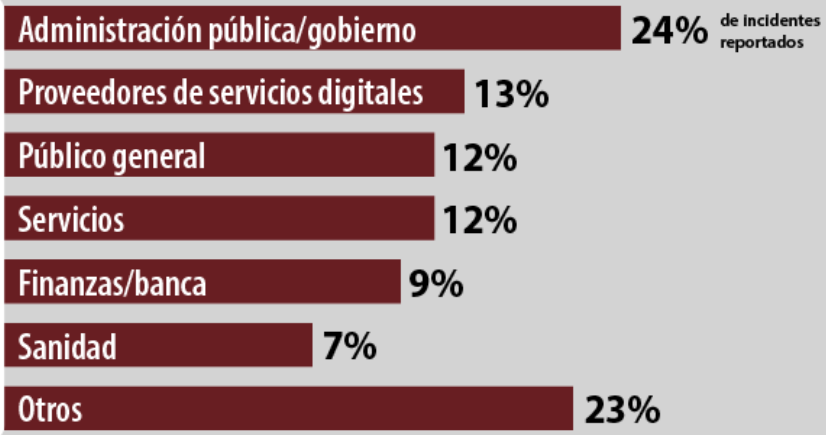
- HAY QUE SER CAPACES DE DISTINGUIR ENTRE:
  - Ciberseguridad
  - Seguridad de la información
  - Seguridad informática

- ¿Cuál es el ámbito de actuación de?:
  - Ciberseguridad
  - Seguridad de la información
  - Seguridad informática

AMENAZAS DE LA SEGURIDAD DE DATOS

LOS 6 SECTORES MÁS AFECTADOS POR LAS AMENAZAS A LA CIBERSEGURIDAD

Porcentaje de incidentes relacionados con las amenazas principales observados entre julio de 2021 y junio de 2022 por la Agencia de la Unión Europea para la Ciberseguridad



Fuente: Agencia de la Unión Europea para la Ciberseguridad (ENISA), 2022

AMENAZAS DE LA SEGURIDAD DE DATOS

¿Qué entendemos por amenaza?

•Cualquier acción mal intencionada o no, que ponga en riesgo la seguridad de los datos

• En una sociedad digital las amenazas crecen exponencialmente.

•TIPOS:

- Amenaza INTERNA
- Amenaza EXTERNA

AMENAZAS DE LA SEGURIDAD DE DATOS

AMENAZAS INTERNAS

- Amenazas INTRA de la organización

- Pueden ser:
  - Amenaza INTERNAS INTENCIONADAS - MALICIOSAS
  - Amenaza INTERNAS POR DESCUIDO

AMENAZAS DE LA SEGURIDAD DE DATOS

AMENAZAS INTERNAS INTENCIONADAS - MALICIOSAS

- Amenazas MALICIOSAS
- EJEMPLOS:
  - Malware interno
  - Abuso de privilegio
  - Sabotaje interno
  - Fugas de datos intencionados
  - Phising interno
  - Robo de propiedad intelectual
  - Daños físicos de equipamiento informático de forma voluntaria
  - ……
- Pueden ser:
  - Colaboradores
  - Lobo solitario

AMENAZAS DE LA SEGURIDAD DE DATOS

AMENAZAS INTERNAS POR DESCUIDO

- Amenaza INTERNAS POR DESCUIDO
  - Gestión de permisos inadecuados
  - Acceso a la información impresa
  - Daños físicos equipamiento de naturaleza involuntaria
  - Peones
  - Goof
  - ¿Se os ocurre alguna más?

AMENAZAS DE LA SEGURIDAD DE DATOS

AMENAZAS INTERNAS

- ¿Cómo detectar una amenaza interna?

  1.- Indicador de comportamiento

  2.- Indicadores digitales

AMENAZAS DE LA SEGURIDAD DE DATOS

AMENAZAS EXTERNAS

- Amenazas EXTRA de la organización

- Pueden ser:
  - RANSOMWARE
  - MALWARE
  - INGENIERIA SOCIAL
  - PHISING Y SMISHING
  - ATAQUES DE HACKING
  - ATAQUES DE DENEGACIÓN DE SERVICIOS
  - ATAQUES DE FUERZA BRUTA
  - ATAQUES CONTRA BASE DE DATOS
  - DESINFORMACIÓN MAL USO DE LA INFORMACIÓN (DeepFake)

AMENAZAS DE LA SEGURIDAD DE DATOS

INGENIERA SOCIAL PHISING SMISHING

RIESGOS ASOCIADOS AL MENEJO DE DATOS SENSIBLES

¿QUE ES EL RIESGO?

- Se refiere a la posibilidad o probabilidad de que ocurra un evento o incidente que afecte negativamente a la seguridad, integridad, o disponibilidad de los datos de la organización.

- Un riesgo puede ser:
  - Violaciones de datos
  - Robo de identidad
  - Ataque de virus
  - Daño reputacional
  - Incumplimiento de las leyes, consecuencias legales

RIESGOS ASOCIADOS AL MENEJO DE DATOS SENSIBLES

DATOS SENSIBLES - ESPECIALES

- Son aquellos que están estrictamente relacionado con los derechos y las libertades fundamentales de las personas cuyo tratamiento puede conllevar riesgos importantes para los derechos y libertades.

- Datos personales: incluyen información que identifican a una persona de manera directa

- Diferencias entre datos sensibles y datos personales

RIESGOS ASOCIADOS AL MENEJO DE DATOS SENSIBLES

TRATAR DATOS SENSIBLES

- El RGPD prohíbe el tratamiento de datos personales sensibles.
- Excepto cuando:
  - Exista consentimiento del interesado
  - Proteger los intereses vitales del interesado
  - El interesado ha hecho manifiestamente público sus datos.
  - El tratamiento lo realiza una organización sin ánimo de lucro con finalidad política, filosófica y religiosa.
  - Cuando el tratamiento este fundamentado en la legislación vigente bajo la responsabilidad de personas sujetas a la obligación de secreto profesional. Para fines de asistencia sanitaria. Para procedimientos judiciales

MEDIDAS OBLIGADAS PARA TRATAR DATOS SENSIBLES

Medidas obligatorias para poder tratar datos sensibles

MEDIDAS OBLIGADAS PARA TRATAR DATOS SENSIBLES

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

- Contenido del registro:
    - Identificador y datos de contacto del DPO, del responsable y del encargado
    - Fines de tratamiento
    - Descripción de las categorías de datos personales del interesado
    - Destinatarios existentes, previstos o a quien se le comunicarán los datos.
    - Transferencias internacionales de datos (si las hubiera)
    - Plazos previstos para la supresión de datos (cuando sea posible)
    - Descripción detallada de las medidas de seguridad adoptar

MEDIDAS OBLIGADAS PARA TRATAR DATOS SENSIBLES

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

- Descripción de medidas técnicas y organizativas de seguridad a adoptar: medidas como

    - La seudonimización y el cifrado de datos
    - La capacidad de garantizar la confidencialidad, integridad y disponibilidad.
    - La capacidad de restaurar
    - Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO	
TRATAMIENTO (indicar el nombre del tratamiento, ejemplo: Tratamiento de Clientes	
NOMBRE DEL RESPONSABLE DEL TRATAMIENTO (O REPRESENTANTE)	
DATOS DE CONTACTO DEL RESPONSABLE	
DATOS DE CONTACTO DEL DELEGADO DE PROTECCION DE DATOS (Si hubiere sido nombrado) (No es necesario señalar el nombre del Delegado)	
FINES DEL TRATAMIENTO (Para que se van a usar los datos, ejemplo en un tratamiento de clientes: Facturar compras, seguimiento de la relación comercial, comunicaciones.	
BASE LEGAL DEL TRATAMIENTO, solo obligatoria cuando se trate de los sujetos a los que se refiere el Art. 77.1 de la LOPDyGDD (recomendable para todos) (las bases legales las encontramos en el art. 6 del RGPD)	
CATEGORIA DE INTERESADOS (Ejemplo: clientes, proveedores, empleados, etc.)	
CATEGORIA DE DATOS PERSONALES (Ejemplo: Datos identificativos, Datos económicos, Imágenes, etc.)	
CATEGORÍAS DE DESTINATARIOS A QUIENES SE COMUNICARON O COMUNICARÁN LOS DATOS PERSONALES	
TRANSFERENCIAS INTERNACIONALES DE DATOS (hay TI cuando se remiten los datos a destinatario fuera del Espacio Económico Europeo (países de la UE más Liechtenstein, Islandia y Noruega) Señalar garantías adecuadas en caso art.49.1 RGPD	
PLAZOS PREVISTOS PARA LA SUPRESIÓN DE LAS DIFERENTES CATEGORÍAS DE DATOS	
DESCRIPCIÓN GENERAL DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD	

REGISTRO ACTIVIDADES DE TRATAMIENTO

Registro tratamiento para cámaras de video vigilancia

Actividad de tratamiento	Videovigilancia
Legitimación de tratamiento	Artículo 6.1.e del RGPD: Cumplimiento de una misión de interés público
Fines del tratamiento	Garantizar la seguridad de personas, bienes e instalaciones
Categorías de datos personales	Imagen
Categorías de afectados	Clientes y trabajadores

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Registro tratamiento gestión de nóminas

Descripción del tratamiento					
Nombre del tratamiento	Gestión de la nómina				
Fecha de creación del registro	01/02/2019				
Fecha de actualización del registro	02/02/2020				
Actores	**Nombre**	**Dirección**	**Páis**	**Teléfono**	**Dirección email**
Responsable	Jose Sánchez	C/ Calle, 1, CP: 28000, Madrid	España	91XXXXXXX	email@ejemplo.com
DPO	Luis López	C/ Calle, 1, CP: 28000, Madrid	España	91XXXXXXX	email@ejemplo.com
Organización del DPO (si es externo)	N/A				
Finalidad del tratamiento					
Finalidad principal	Gestión de nóminas				
Sub-finalidad 1	Cálculo de remuneración				
Sub-finalidad 2	Cálculo del importe de los pagos eviandos a organizaciones sociales				
Sub-finalidad 3	Orden de transferencia al banco				

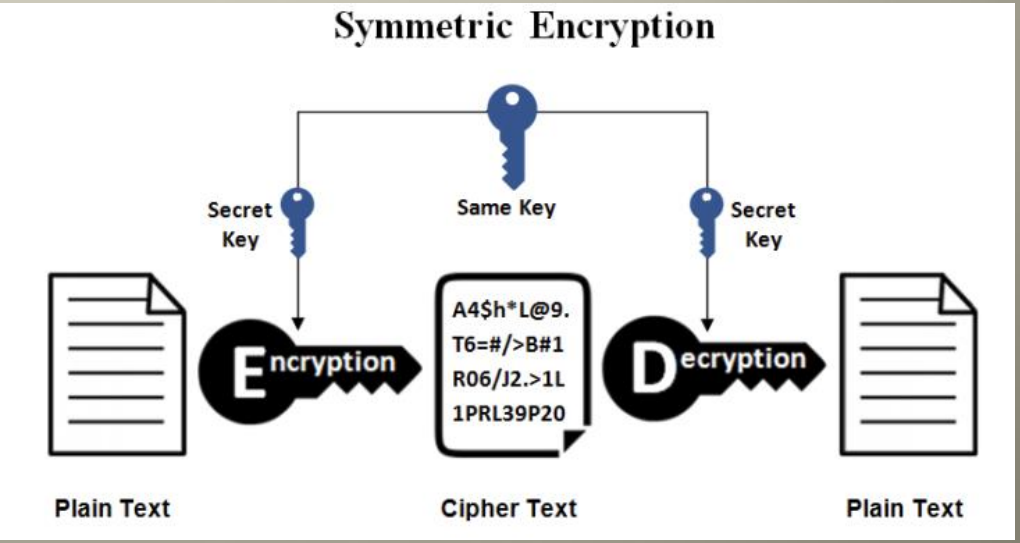
MEDIDAS PARA TRATAR DATOS SENSIBLES

INFORME DE EVALUACIÓN DE IMPACTO DATOS PERSONALES (EIPD)

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

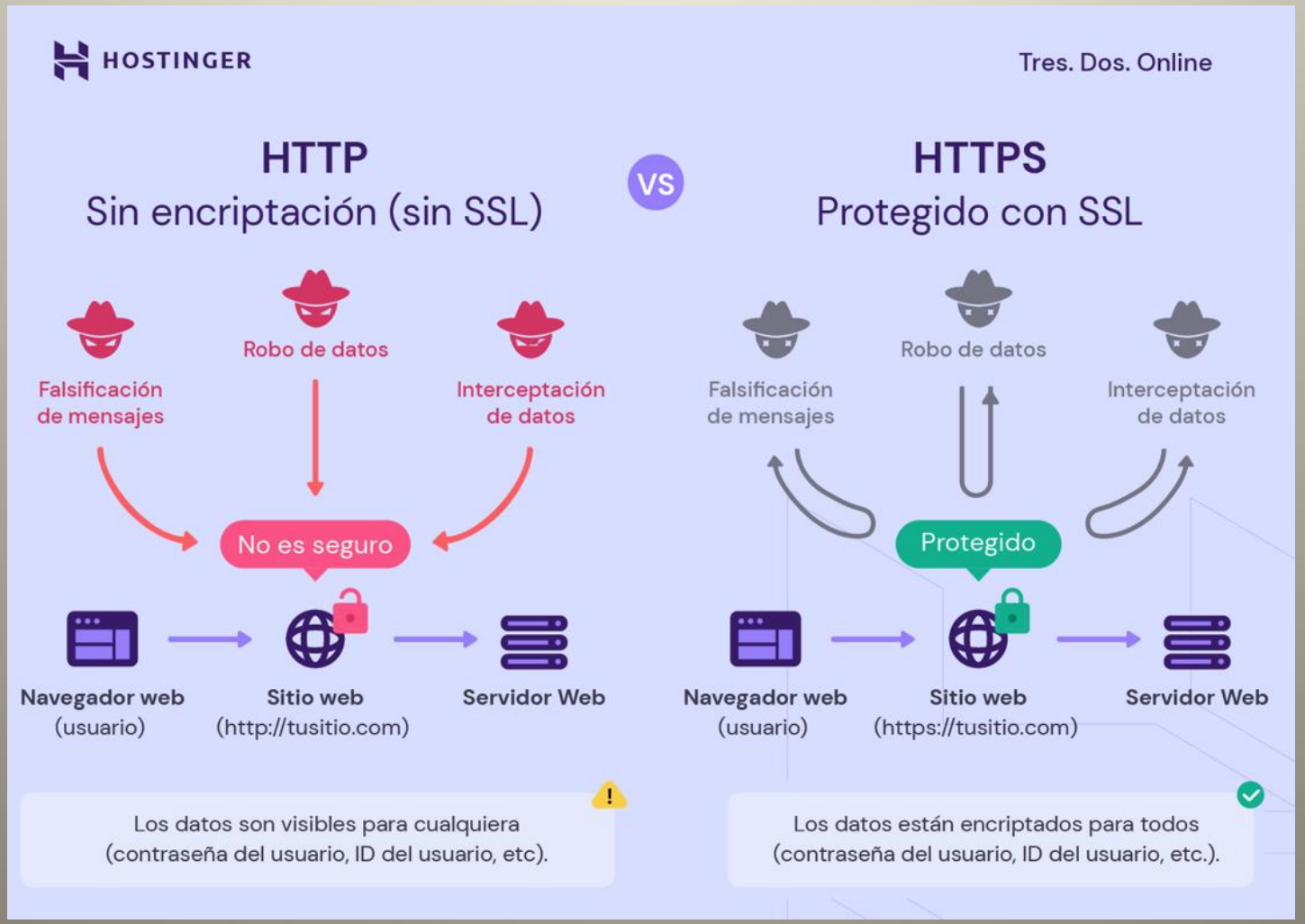
ENCRIPTACIÓN DE DATOS

- Proceso matemático, altera los datos mediante un algoritmo y una clave.
- Encriptación en tránsito
- Encriptación en reposo
- Encriptación simétrica
- Encriptación asimétrica



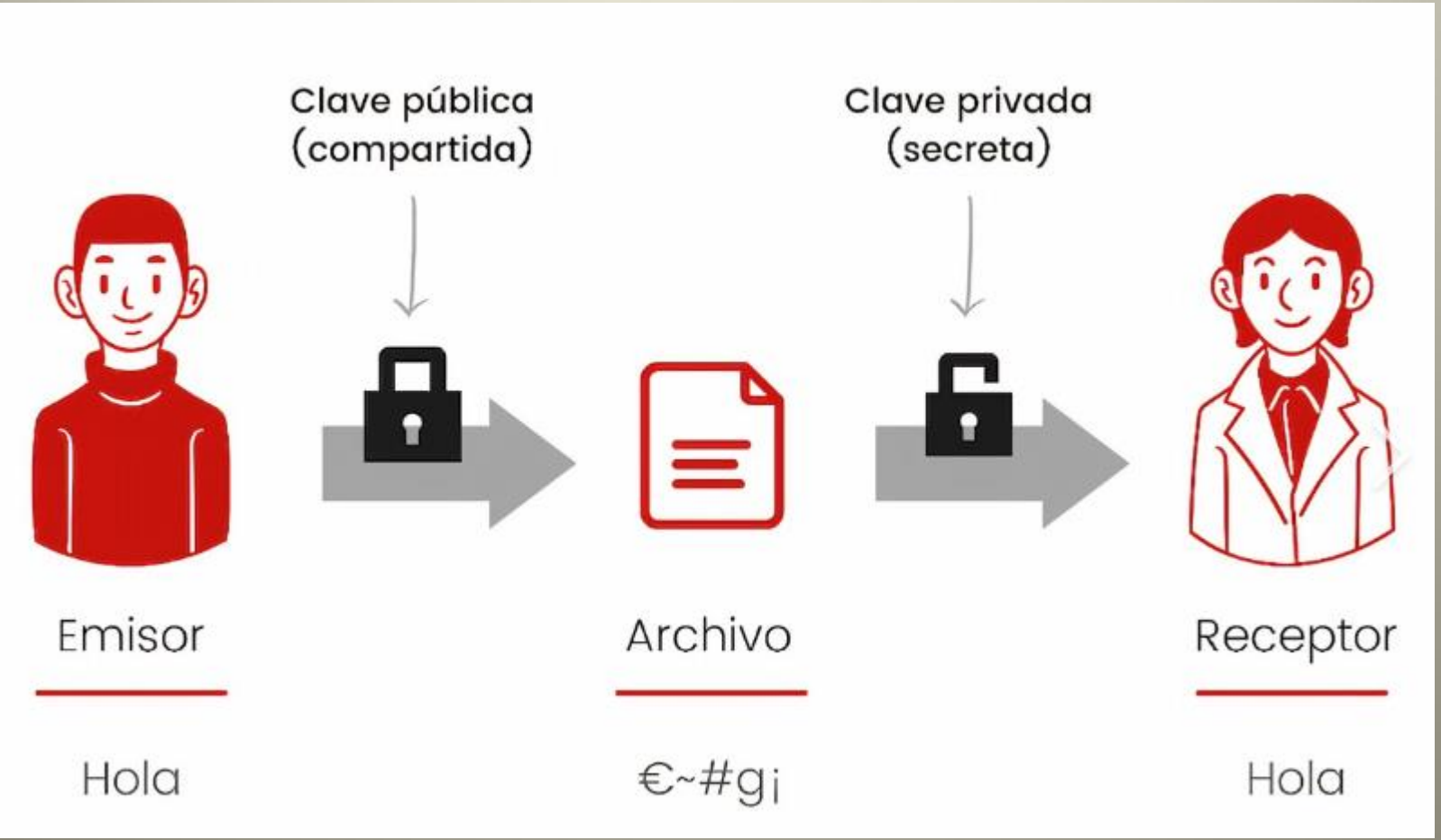
HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

ENCRIPTACIÓN DE DATOS



HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

ENCRIPTACIÓN DE DATOS



HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

ENCRIPTACIÓN DE DATOS

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

OPTIMIZACIÓN DE LA COPIA DE SEGURIDAD Y LA RECUPERACIÓN DE DATOS

- Práctica esencial para garantizar la seguridad de los datos
- Realizar copias de seguridad con frecuencia
- Realizar instantáneas de servidores
- Aplicar la compresión de datos
- Alternar varios métodos de almacenamiento, en la nube, dispositivos externos
- Cifrar los datos de las copias de seguridad
- Realizar pruebas periódicas
- Verificar que las copias son accesibles y se pueden restaurar
- Decidir el periodo de retención

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

DATA MASKING

- Enmascaramiento de datos
- Técnicas de enmascaramiento:
    - La Encriptación
    - Scramble de carácter
    - Sustitución

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

DATA MASKING

TEXTO ORIGINAL	TEXTO ANONIMIZADO	TEXTO SEUDONIMIZADO CON "SUSTITUCIÓN"
Carlos García Atalvio, con NIF 122345678Z, residente en la calle Almagrón, en Alcalá de Henares, Madrid, trabaja en Nymiz Software Company. S.L. Nacido el 12 de Junio de 1980 en Madrid. Carlos García Atalvio es un especialista en Inteligencia Artificial.	**********, con NIF **********, residente en la **********, trabaja en **********. S.L. Nacido el ********** en ******. ********** es un especialista en Inteligencia Artificial.	PER_0001, con NIF IDE_0001, residente en la ADD_0001, trabaja en ORG_0001. S.L. Nacido el DAT_0001 en LOC_0001. PER_0001 es un especialista en Inteligencia Artificial.

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

SEGURIDAD DE ACCESO A DATOS

- Políticas del active directorio GPO
- Estructurar las unidades de red compartida
- Establecer políticas por unidades de servicios y áreas
- Establecer permisos de lectura, escritura y borrado
- Gestión de permisos de acceso a las aplicaciones de la organización (PADRON, CONTABILIDAD)

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

PROMOCIONAR LA TRANSPARENCIA Y LA CULTURA DEL DATO Y PROTECCIÓN

- Formación a los usuarios
- Fomentar, educar en la cultura del dato y seguridad de la información
- Formación en protección de datos
- Ejemplo: FORMAR en la importancia del cambio de contraseña

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

DISPONER DE UN SEGURO CIBERNÉTICO

- Disponer de protección financiera
- Respuesta rápida y confiable
- Cumplimiento normativo

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

IMPLEMENTAR SISTEMAS DE SEGURIDAD PERIMETRAL

- Firewall
- VPN
- Segmentación de redes
- Autentificador de doble factor
- Antivirus
- Antispyware
- Video vigilancia
- Control de accesos (CPD, dependencias)

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

IMPLEMENTAR SISTEMAS DE SEGURIDAD PERIMETRAL

- OBJETIVOS:

- Soportar ataques externos
- Detectar e identificar los ataques recibidos
- Monitorizar (IDS Intrusion Detection System)
- Monitorizar (IPS Intrusion prevention System)

HERRAMIENTAS Y TÉCNICAS DE PROTECCIÓN DE DATOS

BUENAS PRÁCTICAS DE SEGURIDAD PERIMETRAL

- BP1.- Fairwall
- BP2.- Actualizar Mantener los sistemas de SW actualizados
- BP3.- Segmentación de las redes, DMZ
- BP4.- Dotar de IDS y IDP
- BP5.- Autentificador (2FA)
- BP6.-Listas negras
- BP7.-Registro y auditoria de eventos.
- BP8.- Cambio de contraseñas

PLANES DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD

PASOS IMPORTANTES PARA DESARROLLAR UN PLAN

- PLANES: Instrucciones diseñadas para ayudar al personal TI a DETECTAR, RESPONDER y RECUPERARSE de incidentes de seguridad de la red

- Hay que prepararse para los incidentes.

- PASOS PARA DERARROLLAR UN PLAN:
    - Determinar funciones
    - Describir políticas se seguridad
    - Formar al personal
    - Simular incidentes se seguridad
    - Aprender de la experiencia

PLANES DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD

PUNTOS CLAVE PARA IMPLEMENTAR UN PLAN

- Identificar el incidente
- Clasificación del incidente (GRAVEDAD)
- Priorización del incidente.
- Respuesta del incidente
- Cierre del incidente

HABILIDADES DE LOS COMPONENTES DE LOS EQUIPOS DE RESPUESTA

- Gestión
- Conocimientos técnicos
- Habilidades interpersonales
- Trabajo en equipo

MITIGACIÓN DE RIESGOS

PUNTOS CLAVE PARA IMPLEMENTAR UN PLAN

- Es la estrategia de planificación para reducir amenazas
- El objetivo no es el eliminar la amenaza sino prepararse para desastres inevitables

PASOS PARA MITIGAR RIESGOS

- Identificar el riesgo
- Evaluación del riesgo
- Seguimientos de riesgo
- Implementar un plan de mitigación
- Trabajo en equipo

PROCEDIMIENTOS DE NOTIFICACIÓN

- INCIBE (Instituto nacional de ciberseguridad)
- 017
- cert@incibe.es
- Primer organismo español con competencias en materia de ciberseguridad

Muchas gracias