Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

Seguridad de la información en las Administraciónes Públicas

Introducción

En el contexto actual de transformación digital, las AA.PP están cada vez más expuestas a riesgos derivados del uso intensivo de tecnologías de la información. La protección de la información y de los servicios públicos digitales se ha convertido en una prioridad estratégica.

Este seminario tiene como objetivo introducir los fundamentos de la seguridad de la información en el ámbito de las AA.PP., identificar los principales riesgos y amenazas, y explorar estrategias efectivas de prevención y respuesta ante incidentes.

Conceptos clave

La seguridad de la información se basa en tres principios fundamentales:

- Confidencialidad
- Integridad
- Disponibilidad

Conceptos clave

Confidencialidad

Garantiza que **solo** las personas o sistemas autorizados pueden acceder a la información.

En una administración local, los datos de empadronamiento o de licencias de obras deben estar disponibles solo para personal autorizado, las grabaciones de videovigilancia tienen que tener un plazo de conservación, etc.

Conceptos clave

Integridad

Asegura que la información no ha sido alterada de manera no autorizada. Esto implica que los documentos administrativos, resoluciones o registros electrónicos se mantienen intactos y verificables.

Un documento generado y firmado en papel y posteriormente escaneado puede ser fácilmente modificado y en ningún caso ese documento digitalizado tiene valor legal

Conceptos clave

Disponibilidad

Garantiza que la información y los sistemas están accesibles cuando se necesitan.

Una caída del portal de transparencia o de la sede electrónica en pleno periodo de presentación de solicitudes puede provocar un grave perjuicio al ciudadano y comprometer la legalidad de los procedimientos.

Importancia de la protección de datos en las AA.PP

¿Sois conscientes de la cantidad de datos sensibles y datos especialmente protegidos que poseen las entidades locales?

- Padrón municipal, impuestos, sanciones …
- Ayudas sociales, pertenencia a colectivos vulnerables …
- Menores, adopción, ayudas escolares y becas …
- Salud, datos biométricos, videovigilancia …
- Información fiscal, datos bancarios...

¿Pensáis que esta información está realmente protegida?

- Acceso a los equipamientos y protección fuera de la oficina
- Medias técnicas de acceso y protección
- Políticas de seguridad de la información, copias de seguridad
- Auditorías y análisis de riesgos
- Se realizan procesos de capacitación y sensibilización

Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

Amenazas y riesgos

Amenazas y riesgos

Las amenazas a la seguridad en el entorno digital son múltiples y están en constante evolución. Las entidades locales, a pesar de su menor tamaño, no están exentas de sufrir ataques informáticos. Algunas amenazas comunes hacia los sistemas de información de las AA.PP serían:

- Ransomware
- Phishing
- Pérdida o fuga de información

……. Y muchos más

Amenazas y riesgos

Ransomware

Software malicioso que cifra la información y exige un rescate para su liberación.

Jerez de la Frontera en 2021, que paralizó durante días los servicios municipales (tardaron 6 meses en poner de nuevo todo el sistema al 100%) o en 2023, el Ayuntamiento de Sevilla sufrió un ataque de ransomware que paralizó varios servicios electrónicos. Los sistemas quedaron bloqueados y los archivos cifrados, exigiéndose un rescate económico para recuperarlos (en algún medio de comunicación aseguran que pagaron 2.500.000 euros)

Amenazas y riesgos

Phishing

Correos electrónicos fraudulentos que suplantan la identidad de organismos oficiales o de compañeros de trabajo para obtener credenciales o instalar malware.

Una trabajadora del área de recursos humanos de un gran ayuntamiento de CyL recibió un correo que aparentaba venir del Ministerio de Hacienda. Al hacer clic, introdujo sus credenciales en una página falsa. El atacante accedió al sistema de nóminas y casi logra desviar pagos a una cuenta fraudulenta

Amenazas y riesgos

Pérdida o fuga de información

puede deberse tanto a errores humanos como a accesos no autorizados.

En una diputación provincial, un técnico se llevó una copia en USB de expedientes con datos personales para trabajar desde casa. El USB se perdió, y aunque no contenía claves, la fuga de datos personales de menores y familias vulnerables obligó a notificar a la AEPD e iniciar un expediente sancionador.

Amenazas y riesgos

- Errores humanos en la manipulación de bases de datos.
- Falta de copias de seguridad seguras y actualizadas.
- Fallo en infraestructuras tecnológicas críticas (servidores, redes).

Incumplimiento normativo y mala gestión de datos personales (ENS, RGPD, LOPDGDD)

- Tratamiento inadecuado de datos personales sin base legal.
- Falta de medidas de seguridad en bases de datos con información de ciudadanos.
- Uso indebido de cámaras de videovigilancia sin justificación legal.

Dependencia de terceros y vulnerabilidades en la contratación de servicios tecnológicos

- Proveedores sin certificación ENS que no garantizan medidas de ciberseguridad.
- Falta de control en subcontrataciones de servicios cloud o almacenamiento de datos.
- Uso de software sin actualizaciones ni mantenimiento adecuado.

Amenazas y riesgos

Ataques de denegación de servicio (DDoS)

Colapsan servidores para dejar inoperativos servicios como el registro electrónico o la sede.

En marzo de 2025, el portal web del Ayuntamiento de Toledo sufrió un ataque DDoS. Durante varias horas, los ciudadanos no pudieron acceder a la sede electrónica ni consultar el tablón de anuncios digital. Fue atribuido a un grupo prorruso …… peor realmente el atacante había comprado un software por 7 euros con su tarjeta de crédito en una página web


SER
INICIO
DEPORTES
HUMOR
OCIO Y CULTURA
OPINIÓN
PROGRAMAS
PODCASTS
Sociedad
El 99% de los ayuntamientos españoles incumplen la ley de ciberseguridad
Solo 41 municipios han presentado su esquema de protección de datos

Datos del CCN

Ataques con un nivel de complejidad grande y con capacidad real de afectar a la operación de las AA.PP

Periodo	Ciberataques complejos
2022	55 000
2023	107 000
2024	395 000

SOC Castilla y León

2024	19 000 alertas	1 590 incidentes

Estrategias de Prevención y Mitigación

Es necesario adoptar una cultura de seguridad institucional, integrando la seguridad en la planificación, en la toma de decisiones y en los proyectos de digitalización desde el inicio y con el personal adecuadamente formado

Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

Marco legal

Normativa y marco legal

La seguridad en la administración pública no es solo una cuestión técnica, sino también legal. Las entidades públicas están obligadas por ley a proteger los sistemas y la información que gestionan. Entre las normas más relevantes se encuentran:

- Ley 39/2015
- Ley 40/2015
- RD 203/2021
- Reglamento General de Protección de Datos (RGPD)
- Esquema Nacional de Seguridad (ENS)

Normativa y marco legal

• Ley 39/2015, del Procedimiento Administrativo Común: establece la obligación de que los procedimientos administrativos electrónicos se desarrollen con garantías de seguridad, integridad y disponibilidad.

• Ley 40/2015, de Régimen Jurídico del Sector Público: refuerza el principio de interoperabilidad y la necesidad de garantizar la seguridad de las infraestructuras y servicios digitales.

• RD 203/2021, que aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos y detalla las obligaciones y describe las herramientas paras los OO.PP

Normativa y marco legal

- Reglamento General de Protección de Datos (RGPD)

es la normativa europea (UE 2016/679) que regula el tratamiento de los datos personales, garantizando los derechos fundamentales de las personas en relación con su privacidad. Es de obligado cumplimiento desde mayo de 2018 para todas las organizaciones que traten datos de ciudadanos europeos. Establece principios como la licitud, minimización, exactitud, y transparencia, e impone obligaciones como la obtención del consentimiento, la evaluación de riesgos y la notificación de brechas de seguridad. Se complementa en España con la **LOPDGDD** (Ley Orgánica 3/2018).

Normativa y marco legal

- Esquema Nacional de Seguridad (ENS):

Es un marco normativo español que establece los principios y requisitos para garantizar la seguridad de la información en las administraciones públicas. Su objetivo es proteger la confidencialidad, integridad, disponibilidad y trazabilidad de los sistemas. Se basa en medidas organizativas, operativas y técnicas, según el nivel de seguridad requerido. Es de obligado cumplimiento para todas las AAPP y proveedores tecnológicos que traten información pública.

Normativa y marco legal

Decreto 22/2021, de 30 de septiembre

Establece la **Política de Seguridad de la Información y Protección de Datos** para la Administración autonómica: Alinea la política con el ENS, la Ley 39/2015, la Ley 40/2015, el RGPD y la LO 3/2018.

Define responsabilidades, estructura organizativa, criterios de gestión documental, gestión de riesgos, formación, notificación de incidentes, continuidad del negocio, etc.

Servicio de Seguridad de la Información tiene, según la Orden MTD/526/2022, de 27 de mayo (https://gobierno.jcyl.es/web/es/consejerias/servicio-seguridad-informacion.html)

Normativa y marco legal

Cumplir con este marco legal implica no solo contar con herramientas tecnológicas, sino también elaborar políticas de seguridad, planes de continuidad, protocolos de actuación, auditorías y formación del personal.

Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

¿Cómo podemos mejorar la seguridad de la información?

¿Qué podemos hacer (todos)?

NO solo es un tema que afecte a los departamentos de TI, al INCIBE, a la Comunidad Autónoma, Diputación…… **TODO el personal de un OO.PP. puede hace que se mitiguen hasta el 80% de los problemas de seguridad**

Algunos ejemplos típicos:

- Contraseñas débiles o compartidas entre empleados.
- Acceso a documentos confidenciales desde redes públicas o dispositivos no seguros.
- Descarga de archivos adjuntos de correos sospechosos.

¿Qué deberíamos tener (todos)?

Cada **puesto de trabajo** debería de tener:

- **Antivirus y sistemas de detección de intrusiones (IDS/IPS):** protegen contra amenazas conocidas y comportamientos anómalos.
- **Firewalls y segmentación de red**: reducen la exposición a ataques y evitan la propagación lateral dentro de la red.
- **Sistemas de gestión de identidades**: controlan los accesos y privilegios de cada usuario.
- **Cifrado de comunicaciones y almacenamiento**: protege la información frente a interceptaciones.
- **Portafirmas electrónicos y sistemas de archivo seguro**: garantizan la integridad de los documentos administrativos.

¿Qué deberíamos tener las EE.LL.?

Las estrategias para mitigar los riesgos deben ser tanto técnicas como organizativas. Algunas medidas técnicas eficaces incluyen:

- **Segmentación de redes**: separar las redes administrativas internas de las zonas expuestas a Internet.
- **Control de accesos**: políticas de contraseñas, uso de doble factor de autenticación, perfiles y permisos adecuados.
- **Formación continua**: todos los empleados deben ser conscientes de las amenazas y saber cómo actuar ante un correo sospechoso o una brecha de seguridad.
- **Copias de seguridad**: actualizadas, probadas y almacenadas fuera de línea.
- **Plan de respuesta a incidentes**: protocolos claros sobre qué hacer, a quién informar y cómo actuar ante distintos tipos de incidentes.

¿Qué deberíamos tener las EE.LL.?

- Nombramiento de un **Responsable de Seguridad y un Responsable de Protección de Datos** (RPD).
- **Inventario** actualizado de **activos**, datos y aplicaciones.
- **Accesos** definidos por **roles** (mínimos necesarios).
- **Registro** de **accesos** y cambios (logs de trazabilidad).
- **Procedimientos** claros de notificación y **gestión de incidentes**.

Decálogo de la ciberseguridad

Cumple con las normas de seguridad, siguiendo el Esquema Nacional de Seguridad, las políticas de seguridad y protección de datos de la entidad y otras normativas oficiales para proteger los sistemas y la información y

- Usa contraseñas seguras y autenticación doble
- Protege la información confidencial No compartas información sensible o de carácter personal sin autorización. Guarda los documentos con acceso restringido.
- Mantén los sistemas actualizados
- Haz copias de seguridad regularmente y verifica periódicamente que las copias funcionan correctamente.
- Cuidado con las trampas digitales (phishing y estafas)
- Controla quién accede a los sistemas
- Protege los dispositivos y redes y fuera de las instalaciones conectarse a su red con VPN
- Establece un plan de respuesta a incidentes, con un protocolo de actuación en caso de ataque o filtración de datos.
- Revisa la seguridad periódicamente y rrealiza auditorías de seguridad y pruebas de penetración

Enlaces

Guía de Protección de Datos en la Administración Local – AEPD
https://www.aepd.es/guias/guia-proteccion-datos-administracion-local.pdf

Guía de implantación del ENS para entidades locales – CCN-CERT
https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/3758-ccn-stic-883-guia-de-implantacion-del-ens-para-entidades-locales/file.html

Guía "Digitalíza-T!" para Entidades Locales – MINHAP
https://administracionelectronica.gob.es/pae_Home/dam/jcr%3A5d75e090-c719-4d27-8027-ba09451f20fd/GUIA-PARA-EELL-PARA-EL-CUMPLIMIENTO-DIGITAL-DE-LAS-NUEVAS-LEYES-ADMINISTRATIVAS.pdf

Código de Administración Electrónica
https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=29