



**DIPUTACIÓN
DE BADAJOZ**

Jornada Cumplimiento Normativo en Seguridad y Protección de Datos

Recomendaciones básicas seguridad para un Ayuntamiento

05 de Marzo de 2020

sopra  steria



Índice

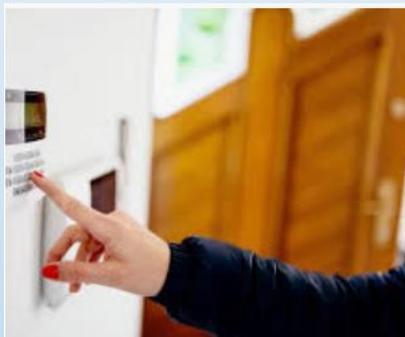
1. Introducción
2. Definiciones
3. Vulnerabilidades
4. La Seguridad de la Información
5. Consejos Básicos de Seguridad de la Información



¿Cómo nos afecta la Seguridad?

Acciones cotidianas que realizamos en nuestro día a día están relacionadas con la seguridad

En casa



En el coche



Viajando



En el banco



Con los
menores
a nuestro
cargo



Vivimos rodeados de Seguridad



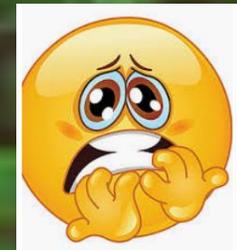
¿Cómo tratamos la información con la que trabajamos?



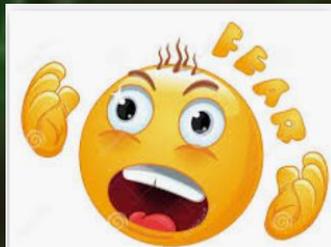
Nunca hubiera imaginado que haciendo clic en un correo fraudulento, todo el sistema de contabilidad se corrompería

LA SEGURIDAD ES RESPONSABILIDAD DE TOD@S

No pensó que una simple Auditoria de seguridad iba a poner en peligro toda su información



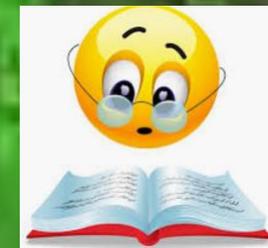
No creía que, al dejar olvidada su DNI en la fotocopiadora, iba a suplantarle su identidad



Hablando de una oferta de trabajo en el tren, no imaginaba que otro viajero me escucharía y sería seleccionado



Acaba de enterarse de que el sistema de información de una empresa externa fue hackeado... ¿el trabajo que me realiza será realmente seguro?



Definamos una serie de conceptos

¿Sabrías definir alguno de los siguientes conceptos?



Amenaza

Acontecimiento que puede producirse, o no, y atentar contra la seguridad



Riesgo

Correlación entre el impacto y la probabilidad de que ocurra una amenaza, atenuada por las medidas de protección



Vulnerabilidad

Debilidad de un bien, o de un conjunto de bienes, susceptible de ser objeto de una amenaza



Comprometimiento *

Divulgación de información confidencial a personas no autorizadas, o sin necesidad de conocerla

** Puede ser de origen interno o externo; voluntario o no*



Definamos una serie de conceptos

Revisemos estos conceptos de forma gráfica



VULNERABILIDADES

Existen 3 tipos de fragilidades de la información:



FÍSICAS

HUMANAS

INFORMÁTICAS



VULNERABILIDADES

Existen 3 tipos de fragilidades de la información:



FÍSICAS

Las fragilidades físicas están relacionadas con el entorno que nos rodea, desde su creación hasta su destrucción pasando por el almacenamiento, el envío... Dentro de este tipo de fragilidades nos encontramos los papeles, tarjetas de accesos...

- Fuego
- Inundación
- Contaminación...



VULNERABILIDADES

Existen 3 tipos de fragilidades de la información:

→ Mala intención:
Robo, vandalismo,
venganza, terrorismo.

→ Imprudencias:
No prever las
consecuencias de
nuestros actos o no
tomar las medidas
necesarias para evitar
estas consecuencias.



HUMANAS

→ Negligencia:
Hacer las cosas con menos
cuidado e interés del
debido.

→ Coacción:
Aprovechar un punto débil
de una persona para
hacerle cometer una
acción ilegítima en
beneficio de un tercero
malintencionado.



VULNERABILIDADES

Existen 3 tipos de fragilidades de la información:

Las fragilidades informáticas son debilidades en el software, o en el hardware, que permita a un atacante comprometer la integridad, disponibilidad, confidencialidad del sistema o de los datos que procesa o contenga

- *Fallos en red*
- *Virus*
- *Denegación del servicio*
- *Defectos de las aplicaciones*
- *Ransomware*



INFORMÁTICAS



2019, año ransomware: 174 ciudades fueron «secuestradas»

En Estados Unidos

Del Rio (Texas)

A principios de año, el ayuntamiento de la ciudad estadounidense Del Río fue atacado por el ransomware. La nota de rescate incluía un número de teléfono para pagar a los atacantes.

Baltimore (Maryland)

7 de mayo de 2019 Baltimore el gobierno municipal cerró la mayoría de sus servidores debido a un ataque de ransomware que afectó a los sistemas de correo utilizados por los empleados municipales, líneas telefónicas o el servicio de pago de facturas online.

Otros municipios estadounidense que ha trascendido que han sufrido ataques por ransomware a lo largo del año han sido:

- Lake City, Riviera Beach y Pensacola (Florida)
- Galt (California)
- Pascagoula (Mississippi)
- Nueva Orleans (Luisiana)



2019, año ransomware: 174 ciudades fueron «secuestradas»

Fuera de Estados Unidos

Otras ciudades que fueron protagonistas, muy a su pesar, por este motivo:



Johannesburgo
(Sudáfrica)



Frankfurt
(Alemania)



En España también contamos con diversos casos sonados:

- Ayuntamientos de Euskadi (Bilbao, Santurtzi,...)
- Zaragoza.
El Instituto de Empleo y Fomento Empresarial sufrió un ransomware que bloqueó sus sistemas informáticos.
- Ayuntamiento de Jerez de la Frontera en Cádiz.



VULNERABILIDADES

Existen 3 tipos de fragilidades de la información:

El **68%** de los comprometimientos se origina dentro de la organización

Verizon Data Breach Investigations Report (DBIR) 2017

El **47%** de los ciberataques dentro de la compañía es llevado a cabo por empleados o exempleados

Informe PriceWaterhouseCoopers (PWC) 2017



FÍSICAS



HUMANAS



INFORMÁTICAS

Las vulnerabilidades humanas son las más sencillas y menos costosas de explotar y constituyen el primer punto del **COMPROMETIMIENTO**



La Seguridad de la Información

La Seguridad de la Información consiste, principalmente, en **PROTEGER** la Disponibilidad, la Integridad, la Confidencialidad y aportar las pruebas (Trazabilidad)

DISPONIBILIDAD

Facilitar la información a los usuarios autorizados cuando la necesitan

INTEGRIDAD

Proteger la información de todo deterioro involuntario o malintencionado

CONFIDENCIALIDAD

Poner la información a disposición únicamente de los usuarios autorizados

TRAZABILIDAD

Poder identificar de manera segura quién ha hecho qué, cuándo y cómo



Consejos Básicos de Seguridad de la Información



Consejos Básicos de Seguridad de la Información

Secreto Profesional y Necesidad de Conocimiento	→	La Ley penaliza el atentado contra la Confidencialidad, la Disponibilidad y la Integridad de los Sistemas de Información.
Protección de Datos Sensibles	→	La protección de la información sensible y de los Datos de Carácter Personal debe ser una constante. La legislación es cada vez más restrictiva.
Normas de Acceso	→	¡Protejámonos! No hay que dejar entrar a los despachos a personas no identificadas y/o desconocidas
Política de Despacho Limpio	→	La discreción sobre la información sensible es necesaria para su protección. No dejéis documentos en impresoras y/o despachos, utilizad destructoras de papel...
Protección del Puesto de Trabajo	→	Realizar las Actualizaciones de Antivirus; Instalar “Patches” Seguridad; NO Abrir Mail Sospechosos... Todos debemos hacer uso responsable de las herramientas.
Derecho de la Propiedad Intelectual	→	Los programas instalados en nuestro puesto de trabajo deben respetar los derechos de licencia, NO deben realizarse descargas ilegales...
Reglas de Uso	→	El uso de los Sistemas de Información debe ser Lícito, Vigilantes, Respetuoso con las condiciones de uso establecidas...
Gestión de Incidentes de Seguridad	→	Frente a un incidente de seguridad tenemos 2 obligaciones: Notificarlo a nuestros responsables + Avisar al buzón de dpdaytos@dip-badajoz.es
Mejora Continua	→	¡TODOS COLABORAMOS! Tanto a nivel individual como a nivel de Ayuntamiento/Mancomunidad como a nivel de Diputación.

DATOS DE CONTACTO

Sara Pacheco Bazaga
Consultora Seguridad

spacheco@dip-badajoz.es
sara.pacheco@soprasteria.com

+34 695 668 728

**Buzón Delegado de
Protección de Datos para
Entidades Locales**

dpsdaytos@dip-badajoz.es



sopra  steria

Gracias!