Manual de buenas prácticas en la seguridad de la información

Indice

1.- Introducción

Las actividades criminales en la red suponen uno de lo delitos más abundantes a nivel mundial.

En los últimos años ha superado en volumen económico al tráfico de drogas.

Ayuda en temas de seguridad para el sector público en España → El **Esquema Nacional de Seguridad (ENS).**

El ENS busca:

- la protección de la información que maneja y los servicios que presta.
- impulsar la gestión continuada de la seguridad.
- Proporcionar buenas prácticas de seguridad.

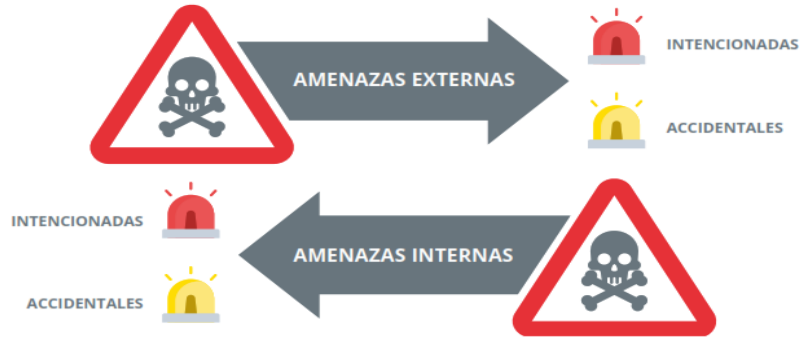
El ENS es **de aplicación a todo el sector público.**

Principios básicos:

- **La seguridad total no existe.**
- **Siempre podemos alcanzar una seguridad razonable.**

2.- Tipos de amenazas

Tipos de amenazas:



2.1 Amenazas externas:

- **Virus**
- Ransomware o secuestro de archivos y documentos, exigiendo un pago o rescate para recuperar el acceso a ellos. Su objetivo es bloquear la actividad de la organización
- Robo de datos bancarios, números de cuenta, tarjetas de crédito
- Robo de información
- **Suplantación de identidad:** Sustracción de datos personales para hacerse pasar por otra persona con fines generalmente económicos, avales crediticios, etc.
- **Sabotaje o vandalismo**
- **Ingeniería Social:** Engaño y suplantación de entidades para obtener nombre, contraseñas y otros datos de carácter personal

¿Cómo detectarlas?

En correos electrónicos:

- La precaución es la primera línea de defensa.
- **Desconfía** de:

- correos mal redactados
- Expresiones extrañas o forzadas
- Sorteos “milagrosos” a los que no nos hemos inscrito
- Supuestas multas que has de tramitar abriendo adjuntos al mensaje de correo
- Supuestos mensajes de urgencia o con carácter apremiante

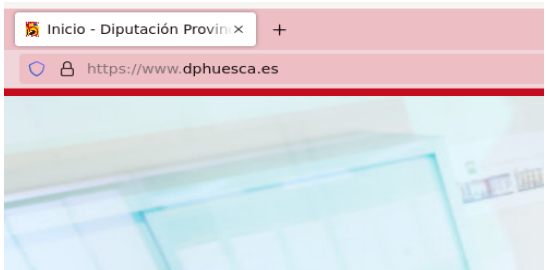
- No reveles información personal en una página que te han enviado a través de correo electrónico.

Otras formas de detectarlas:

- **Comportamiento extraño** de los equipos informáticos.
- Lentitud repentina de los ordenadores.
- Exceso de publicidad o aparición de anuncios dispersos en forma de ventanas emergentes fuera de los navegadores web y sin relación con los mismos
- **Desaparición de documentos** o imposibilidad de acceder a los mismos

¿Qué podemos hacer para evitarlas?

- **Antivirus instalado, activado y actualizado.** Aparecen nuevas amenazas a diario, un antivirus obsoleto es un riesgo
- Sistema operativo **actualizado**
- No abrir **adjuntos de correos** electrónicos de remitentes desconocidos
- **Verificar** que las **webs** a las que accedemos son fidedignas antes de introducir cualquier dato personal y si este se pide por interés legítimo.
  - Que tengan el candadito.



  - Si tenemos dudas, buscar la paǵina web por nuestra cuenta en vez de usar el enlace sospechoso.
- Máxima **precaución** ante el **correo electrónico**: Un banco nunca te pedirá que le des tu numero de tarjeta y su pin correspondiente, al igual que cualquier servicio, jamás te solicitarán tu contraseña.

2.2 Amenazas internas:

- Principalmente **descuidos** o prácticas poco responsables
- Ocasionan daños a la organización por difusión de archivos infectados
- **Sabotajes intencionados** por parte de empleados descontentos.
- Cuidado con las **claves**:
  - ¿Son seguras?
  - ¿No serán compartidas?
  - ¿Las tenemos bien guardadas?

¿Cómo evitar las amenazas internas accidentales?

- Evitar abrir o reenviar documentos de remitentes externos a la organización sin comprobar que se encuentran libres de **virus**.
- Emplear lo menos posible unidades de almacenamiento portátil. Los **USBs** son objetivo de muchos virus.
- Si usamos USBs, que éstos sean verificados por un antivirus, y a ser posible, sean unidades de la organización, aprobadas y certificadas para sus uso.

Gestión de contraseñas

- ¡Contraseñas **robustas**!. Eso no quiere decir que sean imposibles de memorizar, ¡ojo!
- **no** deben comunicarse ni **compartirse** con nadie
- Evitar datos comunes:
  - fechas de nacimiento
  - nombre de familiares
  - el nombre del propio usuario
  - poblaciones habituales
- Cuanto más larga y compleja → ¡más segura!
  - 10 caracteres es el mínimo recomendable
- Complicar los ataques de fuerza bruta y de diccionarios de claves:
  - mezclar mayúsculas y minúsculas
  - poner algún número
  - poner algún caracter especial (?%&@)

- por ejemplo, sustituir las “O” por “.”

Ejemplo:

clave= hipoteca → MAL!!!

clave= hip.TEc4@b4NC. → BIEN!!!

Otras prácticas:

- En caso de que un USB o similar que contuviese información deje de estar en uso, asegurarse que éste ha sido adecuadamente borrado.
  - Una fórmula casera → sobreescribir el USB hasta llenarlo con archivos grandes (por ejemplo, un video copiado todas las veces que quepa).
  - El formateo rápido de un USB **no borra** la información, sólo la oculta. **¡Cuidado!**
    - Es como tirar los papeles a la basura. Los oculta de la mesa, pero ¡no los destruye!

3.- Qué hacer si me han atacado

Si sospecho que mis claves del portal ya no son seguras, debo avisar lo antes posible a los técnicos de la DPH, para que tomen medidas.

Si hay información de origen incierto en mi portal, avisar lo antes posible a los técnicos de la DPH, para que me cambien las claves e investiguen el asunto.

Para contactar con el soporte informático de la Diputación de Huesca, a través de correo gestionweb@dehuesca.es y por teléfono 974 294110.