pimec

Micro, petita i mitjana
empresa de Catalunya

Consejos de
CIBERSEGURIDAD PARA PYMES

pimec.org

HACER COPIAS DE SEGURIDAD

... esto evitará cualquier pérdida de datos por robo, incendio, otros daños físicos o ransomware.

- Una vez **identificado lo que hace falta guardar**, las copias de seguridad tienen que formar parte del día a día de la empresa
- Hacer comprobaciones periódicas a estas copias de que realmente pueden **restaurarse**.
- El dispositivo que contiene la copia de seguridad **no puede estar conectado permanentemente** al dispositivo que contiene la copia original, ni físicamente ni a través de una red local.

FORMAR Y CONCIENCIAR CONTRA LA INGENIERÍA SOCIAL

... mediante la cual se evitarán la mayoría de ataques en que intervenga el factor humano.

- Informarse sobre los **ataques de ingeniería social más habituales**, en que los estafadores solicitan información confidencial.
- Comprobar **signos de engaño evidente en el mensaje**, como ortografía o gramática deficientes, o versiones de logotipos de baja calidad.
- Mantener informados a los trabajadores del peligro de compartir **información personal** en Internet.
- Desactivar la opción de "**compras por Internet**" de totas las tarjetas de crédito de la empresa, y activarlas solo en el momento de realizar un pago.
- **No castigar** al personal que haya sido víctima de un ataque, puesto que otros evitarán informarte en el futuro.

MANTENER SEGUROS LOS TELÉFONOS INTELIGENTES Y TABLETAS

... necesitan todavía más protección que los equipos de escritorio, puesto que se usan fuera de la seguridad de la oficina.

- Utilizar una solución **antivirus** para proteger también estos dispositivos móviles.
- Activar la **protección de acceso para dispositivos móviles**.
- Configurar la **gestión remota** de los dispositivos ayudará a poder localizarlos, bloquearlos o borrarlos de forma remota en caso de pérdida o robo.
- La **actualización automática** mantendrá actualizados los dispositivos y aplicaciones instaladas.
- **Sustituir los dispositivos** que ya no disponen de soporte por parte de los vendedores.
- Utilizar conexiones 3G, 4G o VPN, evitando la conexión en **puntos wifi de acceso público**.

PREVENIR EL DAÑO QUE PUEDAN CAUSAR PROGRAMAS MALICIOSOS (MALWARE)

...mediante la adopción de algunas técnicas simples y de bajo coste.

- Utilizando **antivirus** en todos los dispositivos.
- Instalando solo **programas aprobados y de fuentes conocidas**.
- **Actualizando automáticamente todos los programas y el firmware**.
- Controlando el acceso de **medios extraíbles**, desactivando puertos o limitando el acceso.
- Hay que tener especial cuidado con los **ficheros adjuntos** de correos electrónicos, sobre todo si son ejecutables.
- Activar el **cortafuegos** incluido en el sistema operativo.

UTILIZAR CONTRASEÑAS

... es la forma más básica de evitar que personas no autorizadas accedan a dispositivos y datos.

- Todos los dispositivos deben tener una **contraseña de inicio.**
- Se debe utilizar una **autenticación de doble factor (2FA)** siempre que sea posible.
- Evitar **contraseñas predictibles**.
- Se recomienda utilizar un **gestor de contraseñas**, y asegurarse de que la contraseña maestra es segura.
- Una **contraseña segura** deberá tener números, letras, símbolos, mayúsculas y minúsculas; todo esto en una longitud mínima de ocho caracteres.

Información facilitada por Grail Security Systems.

Fuentes:

- National Cyber Security Centre (NCSC) - Cyber Security: Small Business Guide
- National Institute of Standards and Technology (NIST) - Small Business Cybersecurity Corner
- European Union Agency for Cybersecurity (ENISA) - Security for Small and medium size enterpris

Más información:
Imma Navarra | sistemes@pimec.net