6.2 Protección de dispositivos digitales

En el mundo tecnológico actual, la protección de los dispositivos es imprescindible para garantizar la seguridad de la información. En el camino de garantizar la seguridad de la información no podemos olvidar, entre otras cosas, **proteger nuestros dispositivos digitales**. **Medidas y buenas prácticas** como las que aparecen en la diapositiva, son fundamentales para garantizar la seguridad de los dispositivos digitales en las empresas y para preservar la protección de la información y la reputación de la empresa. Para ello es necesario establecer **controles tecnológicos y organizativos**.

Entre los **controles tecnológicos**, se recomienda el uso de contraseñas fuertes y autenticación de dos factores, así como la instalación y actualización de programas de antivirus y antispyware. La encriptación de datos y la implantación de controles de acceso estrictos son también medidas eficaces para mejorar el nivel de seguridad.

Por otra parte, los controles organizativos exigen el desarrollo e implantación de una política de seguridad y procedimientos claros. Es importante ofrecer a los trabajadores formación y programas de sensibilización en seguridad de la información para reducir riesgos y fomentar conductas seguras que les permitan interiorizar y poner en práctica hábitos de seguridad, trabajando la conciencia digital de los usuarios. Además, conviene realizar auditorías de seguridad e inspecciones periódicas y desarrollar planes de respuesta y gestión ante incidentes.

En los controles organizativos cobra importancia la **protección física de los dispositivos digitales**. Esto obliga a mantener los dispositivos en posiciones seguras y a establecer controles de acceso para evitar que personas no autorizadas lleguen a los dispositivos. Para ello es necesario adoptar las siguientes medidas:

- **Controles de acceso**: Los dispositivos deben ubicarse en lugares con accesos restringidos, como oficinas o zonas de seguridad.
- **Medidas de seguridad**: Para proteger físicamente los dispositivos se pueden utilizar cerraduras, cámaras de seguridad y alarmas.

Protección de Dispositivos en Educación, Trabajo y Vida Diaria

La importancia de la seguridad digital no se limita al ámbito personal; también es fundamental en el ámbito **educativo y laboral.**

En el ámbito educativo, el alumnado y el profesorado deben tener en cuenta la seguridad en el uso de plataformas digitales de aprendizaje. Por ejemplo, antes de descargar archivos deben asegurarse de que no tienen virus y conviene configurar los permisos

adecuados para compartir documentos. Además, es imprescindible conectarse a redes seguras y gestionar la información personal de forma responsable.

En el ámbito laboral, las empresas deben definir políticas claras en cuanto al uso de los dispositivos digitales. El personal debe crear y modificar periódicamente las contraseñas fuertes y controlar el inicio de las últimas sesiones. Las empresas, además, deberían implementar el Plan de Transformación Digital (EDP), formando a sus trabajadores en seguridad digital y estableciendo medidas de protección eficaces.

También como ciudadano es necesario tomar conciencia de la seguridad digital. Por ejemplo, hay que evitar riesgos al utilizar redes públicas Wi-Fi. Al conectarse a los Wi-Fi públicos, los usuarios corren el riesgo de que sus datos sean interceptados y los hackers pueden robar información personal. Para evitarlo, se recomienda utilizar un VPN o no realizar transacciones bancarias a través de la red móvil.

Política de Uso de Dispositivos Digitales en las Empresas

Por otro lado, es imprescindible desarrollar e implantar una política de seguridad y procedimientos claros. Es importante ofrecer a los trabajadores formación y programas de sensibilización en seguridad de la información para reducir riesgos y fomentar conductas seguras que les permitan interiorizar y poner en práctica hábitos de seguridad, **trabajando la conciencia digital de los usuarios**. Además, conviene realizar auditorías de seguridad e inspecciones periódicas y desarrollar planes de respuesta y gestión ante incidentes.

Para proteger los datos de los trabajadores y clientes en las empresas es necesario establecer protocolos claros de seguridad. Una empresa puede adoptar las siguientes medidas para el uso de dispositivos digitales:

- Activación del uso de contraseñas fuertes y autenticación de dos factores.
- Mantener siempre actualizados los sistemas operativos y aplicaciones.
- Instalación de programas antivirus y antispam.
- Utilizar redes wifi privadas y no conectarse a redes públicas.
- Ofrecer sesiones de alfabetización tecnológica al personal para su capacitación en seguridad digital.

Conclusión

La protección de los dispositivos digitales es imprescindible para mantener segura la información personal y profesional. Utilizar contraseñas robustas, actualizar el software, evitar las redes Wi-Fi públicas y mantener activados los antivirus son medidas eficaces para minimizar los riesgos.

Las empresas deberían implantar un Plan de Transformación Digital, formando a sus trabajadores en seguridad digital y desarrollando las políticas adecuadas. En el ámbito educativo y laboral, los usuarios vestidos con seguridad digital tendrán la capacidad de detectar y evitar amenazas. Al fin y al cabo, la ciberseguridad es responsabilidad de todos, y tomando las medidas adecuadas, los dispositivos y los datos se pueden mantener seguros.

(última actualización 20/05/2025)