Castilla-La Mancha

Protección y clasificación de información sensible

CIBER SEGURIDAD

En un mundo cada vez más digitalizado, la protección de la información personal y confidencial es fundamental para prevenir el uso indebido de datos y garantizar la privacidad. Esta guía proporciona recomendaciones prácticas para un manejo seguro y responsable de la información sensible.

Buenas Prácticas

Cifrado de datos

Cifra los datos para garantizar su seguridad, tanto cuando están almacenados (en reposo) como cuando se están transmitiendo (en tránsito).

Uso de contraseñas fuertes

Usa contraseñas fuertes y utiliza doble o múltiple factor de autenticación.

Control de acceso restringido

Controla y limita el acceso a los datos. Únicamente deben acceder aquellos usuarios que lo necesiten.

Política de Privacidad para Datos Sensible

Desarrolla y comunica una política de privacidad clara que explique cómo se manejan los datos sensibles, quién tendrá acceso a ellos y cómo se protegerán.

Consentimiento Explícito en Datos Personales

Obtén el consentimiento explícito de las personas antes de recopilar, almacenar o procesar cualquier información personal, sin olvidar informales de que lo estás haciendo.

Agencia de Transformación Digital de Castilla-La Mancha. 2025

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

Castilla-La Mancha

Clasificación de la información sensible

01 Información de Identificación

Es toda aquella información que permite identificar a una persona: Nombre, apellidos, DNI, dirección, número de teléfono,…

02 Datos Financieros

Es la información relacionada con números de cuentas bancarias, tarjetas de crédito, morosidad o cualquier información relacionada.

03 Información médica

Toda la información relacionada con el estado de salud de una persona. Es considerada información sensible, historiales médicos, resultados de pruebas, etc.

04 Datos Personales sensibles

Representa la información relativa a raza, religión, orientación sexual, afiliación a sindicatos, etc.

Consejos

1. **Verifica siempre**: Asegúrate de que los sitios web, aplicaciones y destinatarios son de confianza antes de entregar información sensible.
2. **Haz copias de seguridad**: No solo protege, también te permite recuperar tu información ante incidentes como pérdida, robo o ataques
3. **Mantente alerta ante fraudes**: Desconfía de correos, mensajes o llamadas sospechosas que soliciten datos personales.
4. **Sé consciente**: La mejor herramienta de seguridad eres tú. Mantente informado y alerta ante posibles riesgos.

Agencia de Transformación Digital de Castilla-La Mancha. 2025

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

Castilla-La Mancha