Gestión de accesos e identidades

Las contraseñas por sí solas ya no son suficientes para garantizar la seguridad de nuestras cuentas y sistemas. Los ciberataques cada vez son más sofisticados, y una sola credencial comprometida puede abrir la puerta a múltiples riesgos. Por eso, es fundamental implementar mecanismos adicionales como la Autenticación Multifactor (MFA), que refuerzan el acceso exigiendo una verificación extra y reducen significativamente las posibilidades de accesos no autorizados.

Autenticación Multifactor (MFA)

Añade una capa extra de seguridad al exigir más de una forma de verificación, como un código temporal o huella digital. Es esencial para proteger servicios críticos.

Principio de Privilegios Mínimos

Cada empleado debe acceder solo a los recursos necesarios para su función. Esto reduce el riesgo en caso de que una cuenta sea comprometida.

Gestión de Cuentas Privilegiadas (PAM)

Las cuentas con altos privilegios deben ser controladas, auditadas y usadas solo cuando sea necesario para evitar abusos y mejorar la trazabilidad.

Ciclo de Vida de las Identidades

Es clave definir y automatizar procesos para crear, modificar y eliminar accesos según los cambios de rol o la salida del personal.

Monitoreo y Auditoría de Accesos

Registrar quién accede a qué y cuándo permite detectar anomalías y responder a tiempo ante incidentes de seguridad.

Capacitación en Seguridad

El personal debe conocer buenas prácticas, como crear contraseñas seguras y detectar intentos de phishing. La formación constante es clave.

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