

Buenas prácticas

En el entorno digital

COLCERT AD-20250709-026

TLP: CLEAR

¿Tu organización sigue buenas prácticas de ciberseguridad?

Una de las medidas más efectivas y sencillas para reducir el riesgo de intrusión es la autenticación multi-factor (MFA). **Este boletín presenta los fundamentos, beneficios y pasos para su implementación exitosa, alineados con estándares internacionales.**



¿Qué es MFA y por qué es clave?

La **MFA** requiere que un usuario proporcione dos o más factores de autenticación antes de conceder acceso a un sistema:



Algo que sabes
(contraseña)



Algo que tienes (token
o app)



Algo que eres
(biometría).

Este enfoque impide que los atacantes accedan solo con contraseñas robadas o adivinadas.

Beneficios de adoptar MFA



- ☐ Protección contra accesos no autorizados incluso en caso de fuga de credenciales.
- ☐ Reducción de incidentes por phishing y malware de robo de credenciales.
- ☐ Cumplimiento de normativas de privacidad y seguridad (como ISO 27001, GDPR).

Guía de implementación (pasos prácticos)

- ☒ **Evaluar sistemas críticos:** priorizar cuentas de administración, correo y acceso remoto.
- ☒ **Seleccionar métodos compatibles:** Apps móviles (Authy, Microsoft Authenticator), tokens físicos, biometría.
- ☒ **Integrar MFA en portales y VPNs:** Usar protocolos estándares como SAML o OAuth.
- ☒ **Capacitar al personal:** Explicar su uso y propósito.
- ☒ **Monitorear adopción y excepciones:** Revisar logs y mantener registros.

Errores frecuentes que debes evitar



- ☐ Implementar solo en el correo sin cubrir otros accesos clave.
- ☐ Confiar únicamente en SMS como segundo factor.
- ☐ No establecer procesos para recuperación segura de cuentas.

Ataques que se pueden evitar con MFA

Multi-Factor Authentication (MFA)		
	Phishing (spear phishing, vishing, smishing) Si el atacante obtiene la contraseña, no podrá iniciar sesión sin el segundo factor (token, app, etc.).	 Ataques automatizados y de fuerza bruta
	Credential Stuffing (relleno de credenciales) Técnica que prueba combinaciones de usuario y contraseña filtradas desde otros servicios. Con MFA, no basta con tener solo la contraseña.	 Phishing dirigido (spear phishing)
	Password Spraying Ataque de fuerza bruta a múltiples cuentas con contraseñas comunes. MFA bloquea el acceso sin el segundo factor	 Keyloggers No podrá capturar un token o código de autenticación dinámico.
	Replay Attacks En ataques donde se capturan credenciales transmitidas, el uso de códigos temporales (OTP/TOTP) hace inútiles esas credenciales.	 Suplantación con credenciales robadas (OTP/TOTP)
	Malware de acceso remoto (RATs) Los accesos maliciosos a cuentas privilegiadas desde sistemas comprometidos son bloqueados por requerir un segundo canal de autenticación.	 Ataques a aplicaciones SaaS / Webmail (O365, Gmail, VPNs)
	Accesos no autorizados por empleados malintencionados Al exigir un token adicional o aprobación biométrica, se reduce la posibilidad de abuso de credenciales internas.	 Manipulación encubierta de cuentas y datos

Buenas prácticas

En el entorno digital

COLCERT AD-20250709-026

TLP:CLEAR

La autenticación multifactor (MFA) refuerza la seguridad al exigir un segundo paso de verificación, más allá de la contraseña. **Esto minimiza ataques comunes como phishing, fuerza bruta, keyloggers y accesos no autorizados desde malware o empleados internos.** Es una defensa clave frente a amenazas modernas y debe ser adoptada en todos los entornos críticos.

Recursos recomendados



OWASP Authentication Cheat Sheet
[NIST SP 800-63B - Digital Identity Guidelines](#)
CIS Controls – IG1: Use MFA

La MFA no es opcional, es una necesidad en seguridad digital.

Es una defensa clave frente a ataques como el phishing, y su implementación fortalece significativamente la postura de seguridad de las organizaciones.



¡Comienza hoy a fortalecer tus accesos!