cylum
CYBERSECURITY AS A SERVICE

8 buenas prácticas para proteger tu pyme de amenazas digitales

Guía práctica

La ciberseguridad ya no es una opción: es una necesidad para la continuidad y reputación de cualquier negocio, por pequeño que sea.

Aplíca estas buenas prácticas y fortalece tu resiliencia frente a incidentes.

Parte del grupo
FACTUM

1. Cambia las contraseñas por defecto y refuérzalas

Las contraseñas que vienen preconfiguradas son un blanco fácil para los atacantes. Sustitúyelas por combinaciones robustas que incluyan letras mayúsculas y minúsculas, números y caracteres especiales. Establece políticas de cambio regular de contraseñas y evita reutilizarlas entre diferentes servicios.

Tip adicional:

Utiliza un gestor de contraseñas para facilitar la gestión segura.

2. Activa la autenticación de doble factor (2FA)

El doble factor de autenticación añade una capa extra de seguridad al acceso remoto a tus sistemas: incluso si alguien roba tu contraseña, no podrá entrar sin el segundo código. Aplícalo en todos los servicios críticos: correo corporativo, paneles de gestión, CRM, etc.

Recomendación:

Da preferencia a aplicaciones autenticadoras (como Google Authenticator) en lugar de SMS.

3. Asegura tu información en la nube

La nube ofrece muchas ventajas, pero también riesgos si no se gestiona correctamente. Antes de subir documentos o datos sensibles, asegúrate de que el proveedor cumple con estándares de seguridad (como cifrado de datos, control de accesos, etc.).

Consejo:

Configura alertas para detectar accesos no autorizados o actividades sospechosas.

4. Controla el acceso de terceros con monitorización continua

Subcontratas, proveedores, técnicos externos... cualquier actor con acceso a tu red puede ser un punto de entrada para un ciberataque. Implanta un sistema de monitorización continua que registre quién entra, desde dónde y con qué permisos.

Clave:

Aplica el principio de mínimo privilegio. Solo deben acceder a lo que necesitan, y nada más.

5. Mantén todos los softwares actualizados

Las actualizaciones corrigen vulnerabilidades que los ciberdelincuentes explotan rápidamente. Ya se trate de tu sistema operativo, aplicaciones ofimáticas o plataformas de trabajo colaborativo, mantén siempre la última versión instalada.

Extra:

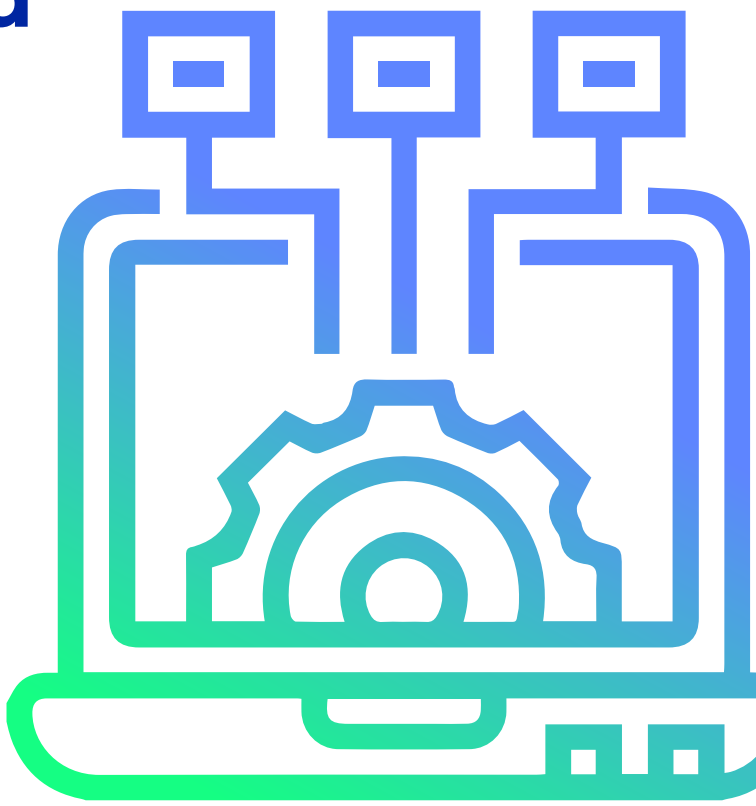
Automatiza las actualizaciones siempre que sea posible.

6. Implementa una política de copias de seguridad

Perder datos es uno de los mayores riesgos para una pyme. Establece una política clara de backups automáticos y verifica regularmente que las copias se están realizando correctamente y que puedes restaurarlas si es necesario.

Regla básica:

Sigue la regla 3-2-1: 3 copias, 2 formatos distintos, 1 en otra ubicación.



7. Aprende a detectar correos sospechosos (phishing)

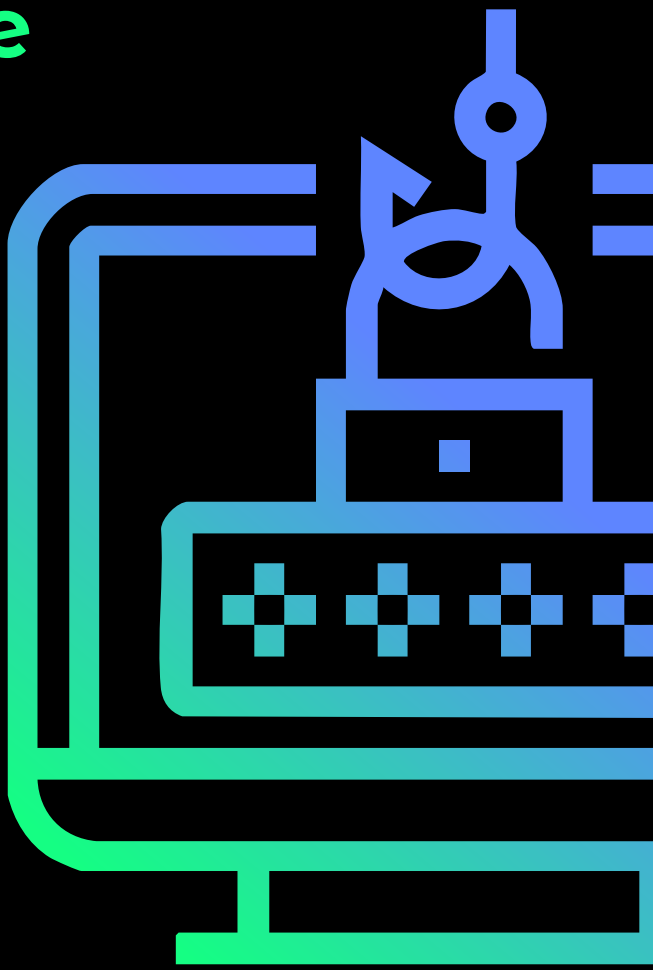
El phishing sigue siendo una de las técnicas más efectivas para engañar a empleados. Enseña a tu equipo a desconfiar de remitentes extraños, enlaces dudosos y archivos adjuntos no solicitados. Ante la duda: no hagas clic.

Sugerencia:

Organiza sesiones breves de formación para empleados con ejemplos reales.

8. Denuncia cualquier incidente de seguridad

Si detectas un ataque o fuga de información, actúa rápido. Informa al INCIBE (Instituto Nacional de Ciberseguridad) o a las Fuerzas y Cuerpos de Seguridad del Estado. La rapidez puede marcar la diferencia entre una simple alerta o una catástrofe.



Importante:

Documenta internamente cada incidente para aprender de él.

Conclusión

La ciberresiliencia no se construye de la noche a la mañana, pero sí con constancia, conciencia y acción. Esta guía te da una hoja de ruta clara para empezar. Adopta estas buenas prácticas y conviértete en una pyme preparada para cualquier reto digital.

Puedes encontrar más contenido como este en www.cylum.tech

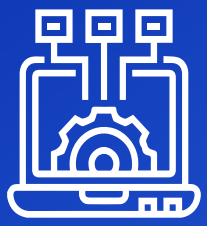
cylum

CYBERSECURITY AS A SERVICE

Simplificamos la ciberseguridad

Soluciona tus necesidades de protección ante riesgos digitales. Cumple con la regulación.

Personal Experto



Tecnología

Cumplimiento normativo

Protección 24x7

Una solución de

FACTUM

15 años protegiendo empresas

www.cylum.tech (+34) 623 425 789 info@cylum.tech