tisec.cl

Ciberseguridad y cumplimiento para PYMEs chilenas

Checklist de Seguridad Básica para PYMEs

Evaluación inicial — 36 controles basados en CIS y Ley 21.663

Usa este checklist para evaluar el estado actual. No te desanimes si hay pendientes: lo importante es tener un punto de partida y priorizar.

IDENTIDAD Y ACCESOS — Nivel: Básico

Control	Hecho	Pendiente	N/A
MFA activado en correo corporativo			
MFA activado en acceso remoto (VPN / escritorio remoto)			
Política de contraseñas documentada y comunicada al equipo			
Gestor de contraseñas corporativo en uso por todo el equipo			
Revisión semestral de usuarios activos y eliminación de cuentas inactivas			
Proceso de revocación de accesos al terminar un empleado (mismo día)			

PROTECCIÓN DE DATOS — Nivel: Básico

Control	Hecho	Pendiente	N/A
Inventario de datos personales que maneja la empresa			
Datos de clientes en sistema con acceso controlado (no en Excel libre)			
Política de privacidad publicada y actualizada en el sitio web			
Formularios de consentimiento actualizados (sin casillas pre-marcadas)			
Contrato con proveedores que acceden a datos de clientes			
Canal para responder solicitudes de titulares (acceso, eliminación)			

BACKUP Y RECUPERACIÓN — Nivel: Básico

Control	Hecho	Pendiente	N/A
Backup automático diario de datos críticos			
Al menos una copia offline o fuera de la red principal (regla 3-2-1)			
Prueba de restauración realizada en los últimos 6 meses			
Backup de correo corporativo activado			
Tiempo de recuperación estimado documentado (RTO definido)			
Backup encriptado o acceso protegido con contraseña			

CORREO Y COMUNICACIONES — Nivel: Intermedio

Control	Hecho	Pendiente	N/A
Registro SPF configurado en el dominio de correo			
DKIM configurado y activo para el dominio			
Política DMARC configurada (mínimo p=none con monitoreo)			
Filtro antispam y antimalware en el servidor de correo			
Capacitación antiphishing para todo el equipo (último año)			
Procedimiento claro de reporte de correos sospechosos a TI			

DISPOSITIVOS Y RED — Nivel: Intermedio

Control	Hecho	Pendiente	N/A
Antivirus/EDR actualizado en todos los equipos corporativos			
Sistema operativo y aplicaciones con actualizaciones automáticas			
Red Wi-Fi corporativa separada de red de invitados			
Equipos corporativos identificados en inventario con responsable			
Política de uso de dispositivos personales (BYOD) documentada			

VPN para acceso remoto a sistemas internos

INCIDENTES Y CUMPLIMIENTO			Nivel: Intermedio
Control	**Hecho**	**Pendiente**	**N/A**
Responsable de seguridad/TI identificado con contacto de emergencia			
Procedimiento de respuesta a incidentes documentado			
Conocimiento del proceso de reporte a ANCI (Ley 21.663, 24 horas)			
Log de incidentes mantenido con cronología y acciones			
Revisión anual de medidas de seguridad en el calendario			
Seguro de ciberseguridad evaluado			

RESUMEN

Total controles: 36 **Hechos: ___ / 36** **Porcentaje: ___ %**

Prioridad 1 (mayor impacto): _____

Prioridad 2: _____

Responsable de implementación: _____ **Fecha objetivo:** _____