CHECKLIST DE CIBERSEGURIDAD

Diagnóstico rápido de tu postura de seguridad

Realizado por: **Simiriki** | Consultores en Ciberseguridad y Automatización

CONTRASEÑAS Y ACCESO

- ■ Tenemos una política clara sobre requisitos de contraseñas
- ■ Las contraseñas se cambian cada 90 días
- ■ Se prohíbe reutilizar las últimas 5 contraseñas
- ■ No hay contraseñas compartidas entre empleados
- ■ Cada usuario tiene credenciales únicas y personales
- ■ Se eliminan cuentas inactivas en menos de 30 días
- ■ Tenemos un registro de quién accede a qué sistemas
- ■ Se requiere MFA para acceso a correo corporativo
- ■ Se requiere MFA para sistemas críticos
- ■ El MFA está habilitado en cuentas administrativas
- ■ Usamos autenticadores seguros (apps, no SMS)
- ■ No todos tienen acceso de administrador
- ■ Se aplica el principio de 'menor privilegio'
- ■ Se revisa periódicamente los permisos elevados
- ■ Los accesos se cambian cuando un empleado se va

EMAIL Y PHISHING

- ■ El correo corporativo tiene filtros anti-spam activos
- ■ Se bloquean automáticamente archivos ejecutables
- ■ El servidor identifica emails externos
- ■ Los links en emails externos se validan
- ■ Los empleados han recibido entrenamiento anti-phishing
- ■ Hacemos simulacros de phishing 2 veces al año
- ■ Los empleados saben reportar emails sospechosos
- ■ Existe un proceso para reportar y analizar intentos

RESPALDOS Y RECUPERACIÓN

- Hacemos respaldos completos al menos una vez a la semana
- Los respaldos están en múltiples ubicaciones
- Se prueban las restauraciones cada 6 meses
- Tenemos documentado dónde están los respaldos
- Hemos creado un plan de recuperación ante desastres
- El plan incluye RTO y RPO definidos

DISPOSITIVOS Y ENDPOINTS

- Todos los dispositivos tienen antivirus actualizado
- El antivirus realiza escaneos automáticos diarios
- Las definiciones de virus se actualizan automáticamente
- Se monitorea la salud del antivirus de forma centralizada
- El SO se actualiza mensualmente o según cronograma
- Las aplicaciones críticas se mantienen actualizadas
- Tenemos un registro de versiones instaladas
- Los discos duros están encriptados
- Los datos en tránsito usan HTTPS/TLS
- Las contraseñas se almacenan encriptadas

RED E INFRAESTRUCTURA

- Tenemos un firewall en el perímetro de la red
- El firewall tiene reglas específicas configuradas
- Se revisan las reglas cada 6 meses
- Existe segmentación entre redes corporativas y críticas
- El WiFi está protegido con WPA3 o WPA2
- Tenemos WiFi separado para visitantes
- Se monitorean los accesos a la red
- Existen alertas para comportamientos anormales
- Existe un registro centralizado de actividad

CUMPLIMIENTO Y POLÍTICAS

- Tenemos políticas de seguridad documentadas

- Las políticas cubren: passwords, email, dispositivos
- Todos los empleados reconocen haber leído las políticas
- Las políticas se actualizan al menos una vez al año
- Existe un proceso definido para reportar incidentes
- Se registran y analizan todos los incidentes

TABLA DE PUNTUACIÓN

Puntuación	Nivel	Interpretación
0–7	CRÍTICO	Vulnerable. Atención inmediata.
8–15	MODERADO	Brechas importantes. Mejora necesaria.
16–20	BUENA	Controles básicos. Refuerza aspectos avanzados.
21+	SÓLIDA	Nivel respetable. Continúa monitoreando.

¿OBTUVISTE UNA PUNTUACIÓN BAJA?

No estás solo. Agenda tu Auditoría Digital Gratuita (1 hora) donde analizamos tu infraestructura y creamos un plan de acción específico.

simiriki.com/diagnostic

Sin costo. Sin compromiso. Solo resultados claros.