LA FIRMA DIGITAL

20 VERIFICACIONES PARA SU EMPRESA

Checklist de ciberseguridad

Una revisión práctica para convertir dudas en acciones.

Empresa: _____

Responsable: _____ Fecha: _____

Cómo utilizarlo

1. Defina qué sedes, sistemas y servicios incluye la revisión.

2. Marque cada punto: C = comprobado, P = parcial, N = no implementado, ? = desconocido, NA = no aplica (justificar).

3. Registre la evidencia y el responsable en su repositorio interno. No copie secretos, datos personales ni configuraciones sensibles en este documento.

4. Lleve los puntos pendientes al plan de acción. Priorice según exposición e impacto, no por la cantidad de casillas completadas.

Alcance: _____

Este documento es una adaptación editorial de La Firma Digital: usa las seis funciones de NIST CSF 2.0 y el enfoque de higiene esencial de CIS. No es el checklist oficial de CIS IG1, ni cubre sus 56 salvaguardas completas.

No asigna un nivel de madurez ni acredita cumplimiento de ISO 27001 u otro estándar. Una casilla marcada exige evidencia; no demuestra ausencia de incidentes.

Verificaciones 1 a 10

Marque: C / P / N / ? / NA. Conserve evidencia fechada por cada punto.

01 GOBERNAR | Responsable de seguridad y decisiones definido.

Evidencia: Nombre, suplente y responsabilidades aprobadas.

Estado: _____ Responsable: _____

02 GOBERNAR | Riesgos priorizados por impacto de negocio.

Evidencia: Registro con responsables y decisiones.

Estado: _____ Responsable: _____

03 GOBERNAR | Proveedores críticos y accesos revisados.

Evidencia: Lista de servicios y condiciones acordadas.

Estado: _____ Responsable: _____

04 IDENTIFICAR | Equipos y aplicaciones inventariados.

Evidencia: Inventario con propietario y fecha de revisión.

Estado: _____ Responsable: _____

05 IDENTIFICAR | Datos sensibles y procesos críticos identificados.

Evidencia: Mapa de ubicación, acceso y criticidad.

Estado: _____ Responsable: _____

06 IDENTIFICAR | Vulnerabilidades registradas y priorizadas.

Evidencia: Registro de hallazgos y acciones pendientes.

Estado: _____ Responsable: _____

07 PROTEGER | MFA aplicado a cuentas sensibles.

Evidencia: Reporte de cobertura y excepciones justificadas.

Estado: _____ Responsable: _____

08 PROTEGER | Privilegios y bajas de usuarios controlados.

Evidencia: Muestra de altas, bajas y revisión de permisos.

Estado: _____ Responsable: _____

09 PROTEGER | Contraseñas únicas y valores de fábrica sustituidos.

Evidencia: Política y verificación; no adjunte contraseñas.

Estado: _____ Responsable: _____

10 PROTEGER | Actualizaciones de seguridad gestionadas.

Evidencia: Reporte de versiones y excepciones.

Estado: _____ Responsable: _____

Verificaciones 11 a 20

Marque: C / P / N / ? / NA. Conserve evidencia fechada por cada punto.

11 PROTEGER | Configuraciones seguras y exposición revisadas.

Evidencia: Revisión autorizada de servicios y reglas.

Estado: _____ Responsable: _____

12 PROTEGER | Datos protegidos mediante cifrado apropiado.

Evidencia: Estado de cifrado y custodia de claves.

Estado: _____ Responsable: _____

13 PROTEGER | Personal formado para reportar sospechas.

Evidencia: Registro de formación y canal de reporte.

Estado: _____ Responsable: _____

14 PROTEGER | Copias de respaldo aisladas y supervisadas.

Evidencia: Reporte de ejecuciones y accesos al respaldo.

Estado: _____ Responsable: _____

15 DETECTAR | Protección de endpoints operativa.

Evidencia: Consola con cobertura y alertas pendientes.

Estado: _____ Responsable: _____

16 DETECTAR | Registros y alertas revisados por un responsable.

Evidencia: Muestra de una alerta investigada.

Estado: _____ Responsable: _____

17 RESPONDER | Plan de incidentes con contactos actualizado.

Evidencia: Plan, responsables y vías de comunicación.

Estado: _____ Responsable: _____

18 RESPONDER | Respuesta ensayada y acciones registradas.

Evidencia: Acta del ejercicio y mejoras acordadas.

Estado: _____ Responsable: _____

19 RECUPERAR | Restauración probada con datos verificados.

Evidencia: Evidencia de prueba y tiempos observados.

Estado: _____ Responsable: _____

20 RECUPERAR | Prioridades y objetivos de recuperación acordados.

Evidencia: Orden de restauración, RTO y RPO por servicio.

Estado: _____ Responsable: _____

De la revisión a la acción

No use una suma de respuestas como calificación de seguridad. Seleccione primero los pendientes que afectan procesos críticos o accesos expuestos.

Prioridad 1 - Punto del checklist: ___ Responsable: _____

Acción: _____

Fecha objetivo: _____ Evidencia de cierre: _____

Prioridad 2 - Punto del checklist: ___ Responsable: _____

Acción: _____

Fecha objetivo: _____ Evidencia de cierre: _____

Prioridad 3 - Punto del checklist: ___ Responsable: _____

Acción: _____

Fecha objetivo: _____ Evidencia de cierre: _____

Próxima revisión: _____ Aprobado por: _____

Referencias oficiales

NIST CSF 2.0 (2024): funciones y gestión de riesgos
https://doi.org/10.6028/NIST.CSWP.29

NIST SP 1300 (2024): guía de inicio para pymes
https://doi.org/10.6028/NIST.SP.1300

CIS Controls v8.1: referencia de controles
https://www.cisecurity.org/controls/v8-1

CIS IG1: priorización de higiene esencial
https://www.cisecurity.org/controls/implementation-groups/ig1

Relación orientativa a nivel de función, no equivalencia normativa: 1-3 Gobernar; 4-6 Identificar; 7-14 Proteger; 15-16 Detectar; 17-18 Responder; 19-20 Recuperar.

¿Necesita priorizar? Solicite una sesión inicial: https://lafirma.digital/diagnostico