

GUÍA PARA CLIENTES EMPRESARIALES

SECURITY CHECKLIST

GUÍA PRÁCTICA PARA EQUIPOS DE
TI Y SEGURIDAD



CYBERSECURITY FRAMEWORK

BY NIST

ÍNDICE

0

OBJETIVO

0

1

IDENTIFY

1

2

PROTECT

2

3

DETECT

3

ÍNDICE

4

RESPOND

4

5

RECOVER

5

6

AWARENESS

6

7

CHECKLIST

7

OBJETIVO

0

Reducir riesgos operativos y de ciberseguridad durante periodos de baja actividad (vacaciones, fin de año), asegurando **continuidad del negocio, protección de datos y capacidad de respuesta ante incidentes.**



I D E N T I F Y

IDENTIFICAR RIESGOS CRÍTICOS

(NIST CSF: ID.AM, ID.RA, ID.BE)

1

ACCIONES CLAVE

Inventariar activos críticos:

- Firewalls, servidores, endpoints, aplicaciones críticas, nube.

Identificar:

- Sistemas legacy o con EOL/EOS.
- Servicios sin soporte activo.

Revisar:

- Dependencias externas (proveedores, MSP, cloud).
- Usuarios con accesos privilegiados.

CHECKLIST

- Inventario de activos actualizado
- Identificación de sistemas críticos de negocio
- Lista de proveedores y contactos de emergencia
- Evaluación rápida de riesgos activos

PROTECT

PROTECCIÓN PREVENTIVA

(NIST CSF: PR.AC, PR.DS, PR.IP, PR.PT)

2

ACCIONES CLAVE

Accesos e identidades:

- Revisar cuentas activas/inactivas.
- Deshabilitar accesos temporales.
- Forzar MFA en accesos remotos y críticos.

Configuración:

- Validar políticas de firewall y VPN.
- Revisar reglas “temporales” o excepciones.

Endpoints:

- Verificar antivirus/EDR activo y actualizado.
- Validar cifrado de discos.

CHECKLIST

- MFA habilitado en accesos críticos
- Cuentas inactivas deshabilitadas
- Reglas de firewall revisadas
- EDR/AV actualizado en todos los equipos

DETECT

MONITOREO Y VISIBILIDAD

(NIST CSF: DE.AE, DE.CM, DE.DP)

3

ACCIONES CLAVE

Logs y monitoreo:

- Confirmar que los logs se están generando y almacenando.
- Verificar retención mínima (30-90 días).

Alertas:

- Validar alertas críticas (login anómalo, malware, VPN).

SOC / Responsables:

- Definir quién monitorea durante vacaciones.

CHECKLIST

- Logs activos en firewall, servidores y nube
- Alertas críticas probadas
- Responsable asignado para monitoreo
- Acceso remoto seguro para el equipo TI

R E S P O N D

4

PREPARACIÓN ANTE INCIDENTES

(NIST CSF: RS.RP, RS.CO, RS.AN | NIST SP 800-61)

ACCIONES CLAVE

Plan de respuesta:

- Validar que el Incident Response Plan esté actualizado.

Contactos:

- Lista clara de escalamiento (TI, dirección, proveedor).

Simulación rápida:

- Qué hacer si ocurre ransomware, caída de VPN o fuga de datos.

CHECKLIST

- Plan de respuesta a incidentes actualizado
- Contactos de emergencia validados
- Roles y responsabilidades definidos
- Procedimiento de comunicación interna listo

RECOVER

CONTINUIDAD Y RECUPERACIÓN

(NIST CSF: RC.RP, RC.IM, RC.CO)

5

ACCIONES CLAVE

Backups:

- Verificar que existan backups recientes.
- Probar restauración (al menos un sistema).

Continuidad:

- Validar RTO/RPO para sistemas críticos.

Documentación:

- Asegurar acceso a diagramas, credenciales seguras y manuales.

CHECKLIST

- Backups recientes verificados
- Prueba de restauración realizada
- Acceso seguro a documentación crítica
- Plan de continuidad validado

AWARENESS

CONCIENTIZACIÓN

(NIST CSF: PR.AT)

6

ACCIONES CLAVE

Enviar comunicado interno:

- Alertar sobre phishing, fraudes y correos falsos.

Recordatorios:

- No usar equipos personales inseguros.
- Evitar Wi-Fi público sin VPN.

Contacto TI:

- Cómo reportar incidentes durante vacaciones.

CHECKLIST

- Comunicado de seguridad enviado
- Canal de reporte activo
- Reglas claras para trabajo remoto

CHECKLIST

RESUMEN RÁPIDO

7

IDEAL PARA **DIRECCIÓN O COMITÉ DE RIESGOS**

- Sistemas críticos protegidos
- Accesos controlados y con MFA
- Monitoreo activo
- Backups verificados
- Plan de respuesta y contactos claros

MARCOS NIST

- **NIST Cybersecurity Framework (CSF 2.0)**
- **NIST SP 800-53** – Controles de seguridad
- **NIST SP 800-61** – Computer Security Incident Handling Guide

CHECKLIST

PRIMERA SECCIÓN

7

1 IDENTIFY

IDENTIFICAR RIESGOS CRÍTICOS

	CONTROL	RESPONSABLE	FECHA
☐	Inventario de activos actualizado		
	Sistemas críticos identificados		
☐	Proveedores y contactos de emergencia		
	Evaluación de riesgos realizada		
☐			
☐			

2 PROTECT

PROTECCIÓN PREVENTIVA

	CONTROL	RESPONSABLE	FECHA
☐	MFA habilitado en accesos críticos		
	Cuentas inactivas deshabilitadas		
☐	Reglas de firewall revisadas		
	EDR // Antivirus actualizado		
☐			
☐			

CHECKLIST

SEGUNDA SECCIÓN

7

3

DETECT

MONITOREO Y VISIBILIDAD



CONTROL

RESPONSABLE

FECHA

Logs activos y con retención

Alertas críticas configuradas

Responsable de monitoreo asignado

4

RESPOND

RESPUESTA A INCIDENTES



CONTROL

RESPONSABLE

FECHA

Plan de respuesta actualizado

Contactos de emergencia validados

Procedimientos de comunicación definidos

CHECKLIST

TERCERA SECCIÓN

7

5

RECOVER

RECUPERACIÓN

	CONTROL	RESPONSABLE	FECHA
☐	Backups verificados		
☐	Prueba de restauración realizada		
☐	Plan de continuidad validado		
☐			
☐			

6

AWARENESS

CONCIENTIZACIÓN

	CONTROL	RESPONSABLE	FECHA
☐	Comunicado de seguridad enviado		
☐	Canal de reporte activo		
☐	Reglas de trabajo remoto comunicadas		
☐			
☐			

CONTACTO

55-39-33-56-60

comercial@networksecurityalliance.com

Canadá 177, San Lucas, Coyoacán,

04030 Ciudad de México, CDMX

