Worry Free

CHECKLIST

Anti-*Ransomware*

cisco Partner

IKUSI velatia

Protege tu empresa hoy mismo con este checklist

El riesgo es real, la solución también

El *ransomware* ha dejado de ser un problema aislado para convertirse en un riesgo sistémico en México. Según datos de ESET, México concentró el 16.3% de las detecciones de *ransomware* en Latinoamérica en 2023, solo detrás de Perú. Además, estudios recientes muestran que más del 60% de las PyMEs mexicanas sufrieron intentos de ataques digitales en 2025, incluyendo *ransomware*, robo de datos y accesos no autorizados.

Estos ataques no distinguen tamaño ni sector, y generan pérdidas económicas, paros operativos y daños reputacionales que muchas veces superan la capacidad de respuesta de las organizaciones.

Frente a este panorama, el checklist de *ransomware* busca ofrecer una herramienta práctica para evaluar el nivel de riesgo de tu empresa y priorizar acciones inmediatas. Identifica el nivel de adopción que tiene tu organización en cada una de las siguientes categorías

1. Gobernanza y Políticas

a. Existencia de una política formal de ciberseguridad

0	1	2	3	4	5

b. Plan de respuesta a incidentes documentado y probado

0	1	2	3	4	5

c. Cumplimiento con normativas locales e internacionales (CNBV, ISO 27001, NIST, GDPR si aplica)

0	1	2	3	4	5

2. Protección de Infraestructura

a. Actualización y parches de sistemas críticos

0 1 2 3 4 5

b. Segmentación de red y control de accesos

0 1 2 3 4 5

c. Uso de EDR/antivirus de nueva generación

0 1 2 3 4 5

3. Gestión de identiddades

a. Autenticación multifactor (MFA) en accesos críticos

0 1 2 3 4 5

b. Gestión de privilegios y cuentas administrativas

0 1 2 3 4 5

c. Monitoreo de accesos sospechosos

0 1 2 3 4 5

4. Respaldo y Recuperación

a. Backups regulares y verificados

0	1	2	3	4	5

b. Almacenamiento de respaldos fuera de línea o en nube segura

0	1	2	3	4	5

c. Pruebas periódicas de restauración

0	1	2	3	4	5

5. Concientización y Capacitación

a. Entrenamiento recurrente a empleados sobre phishing y ransomware

0	1	2	3	4	5

b. Simulacros de ataque (red team/phishing tests)

0	1	2	3	4	5

c. Cultura de reporte inmediato de incidentes

0	1	2	3	4	5

6. Monitoreo y Detección

a. SIEM o SOC activo para detección temprana

0	1	2	3	4	5

b. Alertas automatizadas y correlación de eventos

0	1	2	3	4	5

c. Capacidad de análisis forense interno o externo

0	1	2	3	4	5

7. Relación con terceros

a. Evaluación de proveedores críticos (due diligence de ciberseguridad)

0	1	2	3	4	5

b. Cláusulas contractuales sobre seguridad y notificación de incidentes

0	1	2	3	4	5

c. Monitoreo de integraciones y APIs

0	1	2	3	4	5

Escala de riesgo

0–35 puntos → Riesgo ALTO

El panorama es crítico.

Tu organización carece de políticas formales de ciberseguridad y sus planes de respuesta a incidentes no están probados.
Los respaldos, cuando existen, no se verifican ni se restauran con regularidad, lo que deja a la operación expuesta a pérdidas irreparables.
El acceso a sistemas sensibles suele depender de contraseñas débiles, sin autenticación multifactor, y los empleados rara vez reciben capacitación para reconocer intentos de phishing.

En este escenario, tu empresa se encuentra en un nivel de riesgo alto y necesitas actuar de inmediato.

Soluciones recomendadas:

Cisco Duo

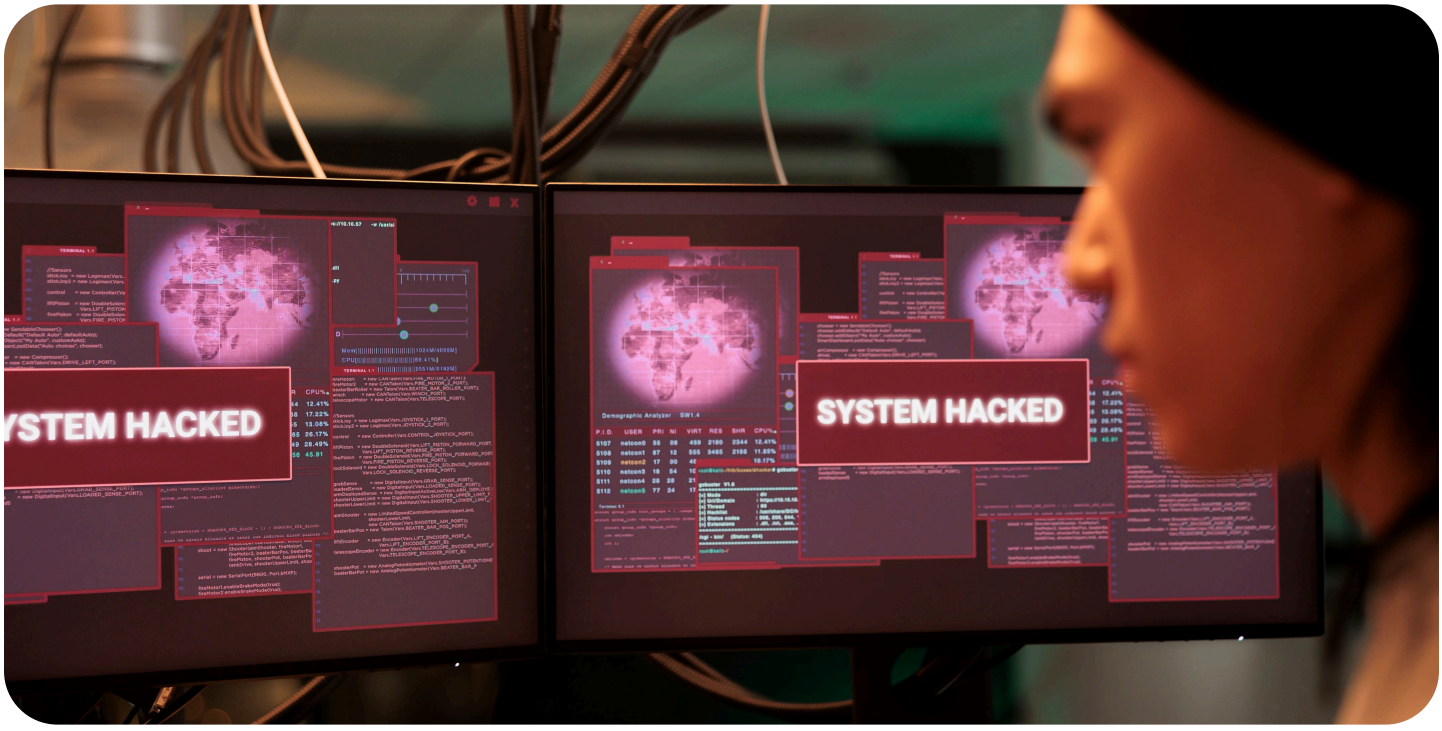
Reforzar accesos críticos con MFA y políticas adaptativas.

Cisco Secure Email Threat Defense

Fortalecer la detección de amenazas en correo y reducir exposición a phishing.

Cisco Umbrella

Analizar archivos en la nube antes de descargarlos y bloquear malware para usuarios dentro y fuera de oficina.



Escala de riesgo

36–55 puntos → Riesgo MEDIO

Tu empresa ya cuenta con algunos controles básicos, pero aún presenta brechas significativas.

Los respaldos existen, aunque no siempre se prueban; la segmentación de red y el monitoreo de accesos son limitados; y la capacitación de empleados es irregular.

Este nivel de riesgo medio refleja una organización que ha avanzado, pero que todavía está lejos de una postura madura de seguridad. En este caso, la prioridad es consolidar lo que ya existe y reforzar las áreas débiles.

Soluciones recomendadas:

Mantener y escalar la estrategia Zero Trust.

Consolidar la protección de correo electrónico como primera línea de defensa.

Controlar qué sitios web y apps usan tus colaboradores remotos sin importar desde dónde se conecten.

Escala de riesgo

56–75 puntos → Riesgo BAJO

Controles robustos, capacidad de respuesta sólida.

Tu organización ya ha documentado y probado sus planes de respuesta, realiza respaldos regulares y verificados, aplica MFA en accesos críticos y fomenta una cultura de reporte inmediato de incidentes.

Además, cuenta con monitoreo activo mediante SIEM o SOC, lo que le permite detectar amenazas en tiempo real.

Aunque el riesgo nunca desaparece por completo, este nivel refleja una organización con una estrategia sólida y resiliente, lista para mantener y escalar esa madurez.

Soluciones recomendadas:

Pasar de la detección reactiva a la búsqueda proactiva de amenazas, reforzando la estrategia Zero Trust.

Consolidar licencias y herramientas, maximizando el retorno de inversión en seguridad.

Blinda la navegación web de tu equipo bloqueando sitios maliciosos automáticamente.

El ransomware seguirá siendo una amenaza persistente en México y las empresas mid-market son un blanco atractivo por su nivel de digitalización y, en muchos casos, por la falta de estrategias de seguridad robustas. Este checklist permite identificar brechas y asignar prioridades, pero la verdadera resiliencia se logra al combinar evaluación constante, capacitación de equipos y soluciones tecnológicas avanzadas.

La integración de **Cisco DUO**, **Cisco Secure Email Threat Defense** y **Cisco Umbrella Secure Access** ofrece un blindaje integral: protección de identidades, accesos y comunicaciones, que reduce drásticamente el riesgo de infección y asegura la continuidad operativa.

En conclusión, la prevención y la respuesta estratégica no son opcionales: son la diferencia entre detener un ataque a tiempo o enfrentar pérdidas irreparables.

¿Buscas un enfoque más personalizado?

Solicita una cita con nuestros expertos y explora como implementar ***Cisco Worry Free*** en tu organización.

Agenda una cita