

● REPORTE DE DIAGNÓSTICO DE CIBERSEGURIDAD NIST CSF 2.0

NexCyber

Empresa Ejemplo, S.A. de C.V.

SECTOR

Manufactura

EMPLEADOS

11 a 50 empleados

DIAGNÓSTICO

Integral

PRÁCTICAS EVALUADAS

48

NIVEL DE MADUREZ

39/100 · BÁSICO

Score limitado a 39 por controles llave · Pocas prácticas implementadas; la exposición es alta.

39/100

Score NexCyber

2 de 7

Controles llave adecuados

29

Brechas identificadas

CONTENIDO DEL REPORTE

02 Resumen ejecutivo

03 Datos de entrada

04 Resultados principales

05 Métricas complementarias

06 Análisis e interpretación

07 Recomendaciones

08 Metodología, fuentes y limitaciones

FOLIO

EJEMPLO-NC-INTEGRAL

FECHA DE GENERACIÓN

15/10/2026 12:00

MOTOR

NexCyber · NexIntelía

• SECCIÓN 02

Resumen ejecutivo

Lo esencial del resultado, en lenguaje claro.

39/100

Score NexCyber

Básico

Nivel de madurez

2 de 7

Controles llave adecuados

29

Brechas identificadas

La empresa evaluada obtiene 39 de 100 en el diagnóstico NexCyber, nivel de madurez Básico. El score se limitó a 39 porque faltan controles llave; atenderlos es lo primero.

Hallazgos clave

- 01** La función más sólida es Detectar con 64 de 100 y la más débil es Recuperar con 28 de 100.
- 02** Controles llave ausentes o apenas iniciados: verificación en dos pasos en correo y nube, respaldos automáticos de información crítica, prueba de restauración.
- 03** Qué atender primero (0–30 días): Paquete de recuperación. Score estimado de 39 a 59 si llega a nivel Mayoritario; atiende 2 controles llave; sube el...

PDF de ejemplo

Empresa y respuestas ficticias, para mostrar el formato del reporte. Las vulnerabilidades mostradas son de demostración.

• SECCIÓN 03

Datos de entrada

Información capturada para generar este reporte.

Empresa

Razón social	Empresa Ejemplo, S.A. de C.V.
Sector	Manufactura
Número de empleados	11 a 50 empleados
Entorno	Servicios en la nube, Trabajo remoto o equipos personales

Cuestionario

Diagnóstico	Integral	Prácticas de nivel Ampliado	No incluidas
Prácticas respondidas	48	Fecha del diagnóstico	15/10/2026 17:58
Respondidas con "no sé"	0		

Datos del Integral

Productos tecnológicos	Palo Alto Networks (PAN-OS), ConnectWise ScreenConnect, PHP
Proveedores críticos declarados	2
Ingreso mensual aproximado	\$2,500,000 MXN
Transferencia grande típica	\$300,000 MXN

Datos declarados

Las respuestas las declaró el usuario y NexIntelía no las verifica: no se accedió a los sistemas de la empresa. El resultado depende de que las respuestas describan la situación real.

SECCIÓN 04

Resultados del diagnóstico

Cifras calculadas por el sistema a partir de tus datos y de fuentes oficiales.

Resultado por función de NIST CSF 2.0

Función	Peso	Prácticas	Score	
Gobernar (GOVERN)	15%	9	51	
Identificar (IDENTIFY)	15%	6	63	
Proteger (PROTECT)	30%	23	50	
Detectar (DETECT)	15%	3	64	
Responder (RESPOND)	10%	4	56	
Recuperar (RECOVER)	15%	3	28	

NIST CSF 2.0 organiza la ciberseguridad en seis funciones: Gobernar (dirección y reglas), Identificar (saber qué se tiene y qué riesgos hay), Proteger, Detectar, Responder y Recuperar. El peso indica cuánto influye cada función en el score general; Proteger pesa más porque reúne las prácticas que evitan los ataques más comunes.

Score limitado por controles llave

Sin el tope, el resultado habría sido 52 de 100. Con controles llave ausentes o apenas iniciados, el score no puede pasar de 39: una empresa sin verificación en dos pasos, sin respaldos aislados o sin parcheo de equipos expuestos sigue muy expuesta aunque tenga otras prácticas en orden.

Controles llave

Control llave	Estado declarado	Semáforo
PR-01 Verificación en dos pasos en correo y nube	No implementado	ATENDER YA
PR-02 Verificación en dos pasos en accesos remotos y de administrador	Mayoritario	ADECUADO
PR-12 Respaldos automáticos de información crítica	No implementado	ATENDER YA
PR-13 Copia de respaldo aislada o inmutable	Mayoritario	ADECUADO
PR-15 Parcheo urgente de equipos expuestos a internet	Parcial	REFORZAR
PR-18 Protección contra malware supervisada	Parcial	REFORZAR
RC-01 Prueba de restauración	No implementado	ATENDER YA

Riesgos principales

#	Práctica con brecha	Función	Estado	Severidad
1	PR-01 Verificación en dos pasos en correo y nube · control llave	Proteger	No implementado	CRÍTICA
2	PR-12 Respaldos automáticos de información crítica · control llave	Proteger	No implementado	CRÍTICA
3	RC-01 Prueba de restauración · control llave	Recuperar	No implementado	CRÍTICA
4	PR-15 Parcheo urgente de equipos expuestos a internet · control llave	Proteger	Parcial	CRÍTICA
5	PR-14 Actualizaciones de sistemas y aplicaciones	Proteger	Iniciado	ALTA

• SECCIÓN 05

Plan de acción, vulnerabilidades y escenarios

Indicadores adicionales y qué indica cada uno.

Plan de acción por plazos

0–30 días · 6 acciones

Práctica	Acción sugerida	Función	Esfuerzo
PR-01 Verificación en dos pasos en correo y nube Sube de prioridad: escenario de fraude por correo con probabilidad Alta (rango medio \$300,000 MXN)	Activar el MFA obligatorio en correo y nube para todos los usuarios. Listo cuando: 100 % de los usuarios con MFA obligatorio, sin excepciones permanentes; métodos resistentes a phishing para administradores.	Proteger	Bajo
PR-12 Respaldos automáticos de información crítica Sube de prioridad: escenario de ransomware con probabilidad Media (rango medio \$1,317,000 MXN)	Configurar respaldos automáticos de todos los sistemas críticos, incluidos los de la nube. Listo cuando: Respaldos automáticos de todos los sistemas críticos, con frecuencia alineada al objetivo de pérdida máxima de datos.	Proteger	Medio
RC-01 Prueba de restauración Sube de prioridad: escenario de ransomware con probabilidad Media (rango medio \$1,317,000 MXN)	Programar una prueba de restauración cada semestre y documentar el tiempo. Listo cuando: Prueba semestral exitosa de los sistemas críticos, con tiempo medido contra el objetivo.	Recuperar	Bajo
PR-15 Parcheo urgente de equipos expuestos a internet Sube de prioridad: 3 vulnerabilidades explotadas en productos declarados, 2 con uso en ransomware	Definir un plazo máximo de 7 días para corregir fallas explotadas en equipos expuestos a internet. Listo cuando: Fallas explotadas activamente corregidas o mitigadas en 7 días o menos.	Proteger	Medio
PR-14 Actualizaciones de sistemas y aplicaciones Sube de prioridad: 3 vulnerabilidades explotadas en productos declarados, 2 con uso en ransomware	Activar las actualizaciones automáticas y revisar cada mes los equipos rezagados. Listo cuando: Al menos el 95 % de los equipos al día; actualizaciones críticas en 30 días o menos.	Proteger	Bajo
RC-03 Plan de recuperación del negocio	Redactar un plan de recuperación para los sistemas críticos con orden de restauración y responsables. Listo cuando: Plan aprobado y revisado en los últimos 12 meses.	Recuperar	Medio

31–90 días · 8 acciones

Práctica	Acción sugerida	Función	Esfuerzo
GV-08 Cláusulas de seguridad con proveedores Sube de prioridad: 2 proveedores críticos casi sin cláusulas de seguridad	Preparar un anexo de seguridad estándar y negociarlo en las próximas renovaciones. Listo cuando: Todos los proveedores críticos con anexo de seguridad firmado.	Gobernar	Medio
PR-09 Capacitación por rol (TI y pagos) Sube de prioridad: escenario de fraude por correo con probabilidad Alta (rango medio \$300,000 MXN)	Establecer la regla de confirmar por teléfono los cambios de cuenta bancaria y capacitar a finanzas y TI. Listo cuando: Capacitación anual por rol y regla de doble verificación de pagos aplicada.	Proteger	Bajo
ID-03 Inventario de datos sensibles Sube de prioridad: escenario de vulneración de datos personales con probabilidad Alta	Elaborar un inventario de datos personales y confidenciales y clasificarlos. Listo cuando: Inventario de datos con ubicación, responsable, clasificación y acceso.	Identificar	Medio
PR-18 Protección contra malware supervisada	Desplegar una solución administrada centralmente (de preferencia EDR) en todos los equipos. Listo cuando: 100 % de cobertura con consola central; de preferencia una solución con detección por comportamiento (EDR).	Proteger	Medio
DE-01 Atención diaria de alertas de seguridad	Asignar a un responsable o contratar un servicio de monitoreo que revise las alertas cada día. Listo cuando: Responsable asignado (interno o proveedor) con revisión diaria y registro de atención.	Detectar	Medio
RS-01 Plan de respuesta a incidentes	Redactar un plan breve con guías para ransomware, fraude por correo y robo de cuenta. Listo cuando: Plan aprobado, revisado en los últimos 12 meses y conocido por los responsables.	Responder	Bajo
PR-04 Mínimo privilegio y cuentas de administrador separadas	Retirar los permisos de administrador del uso diario y crear cuentas administrativas separadas. Listo cuando: Ningún usuario de uso diario con permisos de administrador; cuentas administrativas separadas y registradas.	Proteger	Bajo
PR-22 Seguridad del correo electrónico Sube de prioridad: escenario de fraude por correo con probabilidad Alta (rango medio \$300,000 MXN)	Configurar SPF, DKIM y DMARC y activar el filtrado avanzado del correo. Listo cuando: Filtro activo y DMARC en modo de cuarentena o rechazo.	Proteger	Bajo

91–180 días · 10 acciones

Práctica	Acción sugerida	Función	Esfuerzo
GV-06 Seguridad al contratar y al dar de baja	Crear una lista de verificación de altas y bajas coordinada entre Recursos Humanos y TI. Listo cuando: Lista de verificación aplicada en cada alta y baja; accesos retirados en menos de 24 horas.	Gobernar	Bajo
PR-23 Registros de actividad	Activar y conservar los registros de acceso de correo, nube y servidores críticos. Listo cuando: Registros activados en todos los sistemas críticos, conservados 90 días o más.	Proteger	Bajo
RS-02 Contención rápida	Documentar los pasos de aislamiento y verificar que las herramientas lo permitan. Listo cuando: Procedimiento y herramientas que permiten aislar en menos de una hora, probados.	Responder	Bajo
ID-04 Sistemas críticos del negocio	Identificar los 5 a 10 sistemas críticos y a qué procesos del negocio soportan. Listo cuando: Lista de sistemas críticos con el proceso que soportan y su dueño.	Identificar	Bajo
GV-03 Obligaciones legales y contractuales	Elaborar un registro de obligaciones y actualizar el aviso de privacidad conforme a la LFPDPPP de 2025. Listo cuando: Registro de obligaciones documentado, revisado cada año, y aviso de privacidad vigente conforme a la ley actual.	Gobernar	Bajo
PR-03 Cuentas personales e intransferibles	Eliminar las cuentas compartidas y ligar la baja de cuentas al proceso de Recursos Humanos. Listo cuando: Sin cuentas compartidas para personas; bajas aplicadas en menos de 24 horas.	Proteger	Bajo
PR-20 Firewall y red de invitados separada	Revisar las reglas del firewall y separar la red de invitados. Listo cuando: Firewall con reglas revisadas cada semestre y red de invitados aislada.	Proteger	Bajo
GV-02 Política de seguridad aprobada	Redactar una política breve (3 a 5 páginas), aprobarla en dirección y comunicarla con acuse. Listo cuando: Política aprobada, revisada en los últimos 12 meses y con acuse de lectura del personal.	Gobernar	Bajo
PR-07 Capacitación anual en seguridad	Implementar una capacitación anual breve y obligatoria, más un módulo de inducción. Listo cuando: 100 % del personal capacitado en los últimos 12 meses, incluidos los de nuevo ingreso.	Proteger	Bajo
PR-11 Cifrado en tránsito	Verificar los certificados de todos los servicios y definir canales seguros para enviar información sensible. Listo cuando: Todos los servicios expuestos con cifrado vigente y regla de envío seguro aplicada.	Proteger	Bajo

181–365 días · 5 acciones

Práctica	Acción sugerida	Función	Esfuerzo
PR-25 Trabajo remoto y equipos personales	Definir reglas de trabajo remoto y limitar el acceso desde equipos no administrados. Listo cuando: Reglas documentadas y aplicadas técnicamente.	Proteger	Bajo
RS-04 Apoyo externo de respuesta	Identificar y acordar condiciones con un proveedor de respuesta a incidentes. Listo cuando: Proveedor identificado, con contacto disponible las 24 horas y condiciones acordadas.	Responder	Bajo
ID-07 Alertas de fabricantes y fuentes oficiales	Suscribirse a las alertas de los fabricantes clave y activar las alertas de NexCyber. Listo cuando: Suscripción a alertas de los fabricantes clave y responsable de revisarlas cada semana.	Identificar	Bajo
GV-09 Revisión de la dirección	Incluir la ciberseguridad en la agenda de dirección dos veces al año con el reporte de NexCyber. Listo cuando: Revisión semestral documentada con decisiones y responsables.	Gobernar	Bajo
GV-05 Presupuesto de ciberseguridad	Definir una partida anual de ciberseguridad a partir del plan de acción. Listo cuando: Partida definida, justificada por los riesgos y revisada anualmente.	Gobernar	Bajo

Dentro de cada plazo, las prácticas van en orden de prioridad. La prioridad sube con vulnerabilidades explotadas en sus productos, escenarios de pérdida más probables y proveedores críticos con alerta. Las recomendaciones agrupan estas prácticas en paquetes.

Detalle por práctica

Práctica	Estado declarado	Score	NIST CSF 2.0
GV-01 Responsable de ciberseguridad	Mayoritario	75	GV.RR-02
GV-02 Política de seguridad aprobada	Parcial	50	GV.PO-01
GV-03 Obligaciones legales y contractuales	Iniciado	25	GV.OC-03
GV-04 Evaluación periódica de riesgos	Completo y revisado	100	GV.RM-06
GV-05 Presupuesto de ciberseguridad	Parcial	50	GV.RR-03
GV-06 Seguridad al contratar y al dar de baja	No implementado	0	GV.RR-04
GV-07 Inventario de proveedores críticos	Mayoritario	75	GV.SC-04
GV-08 Cláusulas de seguridad con proveedores	Iniciado	25	GV.SC-05
GV-09 Revisión de la dirección	Parcial	50	GV.OV-03
ID-01 Inventario de equipos	Mayoritario	75	ID.AM-01
ID-02 Inventario de software y servicios en la nube	Mayoritario	75	ID.AM-02
ID-03 Inventario de datos sensibles	Parcial	50	ID.AM-07
ID-04 Sistemas críticos del negocio	Iniciado	25	ID.AM-05
ID-06 Búsqueda de vulnerabilidades	Completo y revisado	100	ID.RA-01
ID-07 Alertas de fabricantes y fuentes oficiales	Parcial	50	ID.RA-02
PR-01 Verificación en dos pasos en correo y nube · llave	No implementado	0	PR.AA-03
PR-02 Verificación en dos pasos en accesos remotos y de administrador · llave	Mayoritario	75	PR.AA-03
PR-03 Cuentas personales e intransferibles	Iniciado	25	PR.AA-01
PR-04 Mínimo privilegio y cuentas de administrador separadas	Parcial	50	PR.AA-05
PR-05 Contraseñas robustas y gestor de contraseñas	Mayoritario	75	PR.AA-01
PR-06 Revisión periódica de accesos	Mayoritario	75	PR.AA-05
PR-07 Capacitación anual en seguridad	Parcial	50	PR.AT-01
PR-09 Capacitación por rol (TI y pagos)	Iniciado	25	PR.AT-02
PR-10 Cifrado de laptops y celulares	Completo y revisado	100	PR.DS-01
PR-11 Cifrado en tránsito	Parcial	50	PR.DS-02
PR-12 Respaldos automáticos de información crítica · llave	No implementado	0	PR.DS-11
PR-13 Copia de respaldo aislada o inmutable · llave	Mayoritario	75	PR.DS-11
PR-14 Actualizaciones de sistemas y aplicaciones	Iniciado	25	PR.PS-02

Práctica	Estado declarado	Score	NIST CSF 2.0
PR-15 Parcheo urgente de equipos expuestos a internet · llave	Parcial	50	PR.PS-02
PR-16 Equipos y software sin soporte	Mayoritario	75	PR.PS-02
PR-17 Configuración segura de equipos	Mayoritario	75	PR.PS-01
PR-18 Protección contra malware supervisada · llave	Parcial	50	PR.PS-05
PR-20 Firewall y red de invitados separada	Iniciado	25	PR.IR-01
PR-21 Sin servicios administrativos expuestos	Completo y revisado	100	PR.IR-01
PR-22 Seguridad del correo electrónico	Parcial	50	PR.PS-01
PR-23 Registros de actividad	No implementado	0	PR.PS-04
PR-24 Seguridad física y borrado seguro	Mayoritario	75	PR.AA-06
PR-25 Trabajo remoto y equipos personales	Iniciado	25	PR.IR-01
DE-01 Atención diaria de alertas de seguridad	Parcial	50	DE.AE-02
DE-02 Alertas de accesos inusuales a correo y nube	Mayoritario	75	DE.CM-03
DE-03 Canal para reportar incidentes	Mayoritario	75	RS.MA-02
RS-01 Plan de respuesta a incidentes	Parcial	50	RS.MA-01
RS-02 Contención rápida	Iniciado	25	RS.MI-01
RS-03 Avisos ante una vulneración	Completo y revisado	100	RS.CO-02
RS-04 Apoyo externo de respuesta	Parcial	50	RS.MA-01
RC-01 Prueba de restauración · llave	No implementado	0	RC.RP-03
RC-02 Objetivos de recuperación	Mayoritario	75	RC.RP-02
RC-03 Plan de recuperación del negocio	Iniciado	25	RC.RP-01

Vulnerabilidades explotadas activamente en sus productos

Productos declarados: Palo Alto Networks (PAN-OS), ConnectWise ScreenConnect, PHP. **Ventana:** vulnerabilidades agregadas al catálogo en los últimos 24 meses.

CVE / producto	Vulnerabilidad y acción requerida (texto de CISA, en inglés)	Agregada	EPSS	Ransomware
CVE-2024-4577 PHP	PHP-CGI OS Command Injection Vulnerability Aplicar las actualizaciones del fabricante.	2024-06-12	N/D	Sí
CVE-2024-1709 ConnectWise ScreenConnect	ConnectWise ScreenConnect Authentication Bypass Vulnerability Aplicar las actualizaciones del fabricante.	2024-02-22	N/D	Sí
CVE-2024-3400 Palo Alto Networks (PAN-OS)	Palo Alto Networks PAN-OS Command Injection Vulnerability Aplicar las mitigaciones del fabricante o discontinuar el producto si no hay mitigación.	2024-04-12	N/D	No conocido

Fuente: Datos de demostración (PDF de ejemplo) — no corresponden a una consulta real. Fecha del catálogo: demostración.

El catálogo KEV de CISA lista vulnerabilidades que ya se están explotando en ataques reales. Que aparezcan aquí no significa que su equipo esté afectado: depende de la versión que use. EPSS estima la probabilidad de explotación en los próximos 30 días.

Escenarios de pérdida

Escenario	Probabilidad relativa	Rango estimado (bajo · medio · alto)	Factores que la elevan
Ransomware o paro de sistemas	MEDIA	\$643,000 MXN · \$1,317,000 MXN · \$2,900,000 MXN Interrupción supuesta: 7, 14 y 30 días (preparación deficiente)	• Verificación en dos pasos en correo y nube (no implementado) • Parcheo urgente de equipos expuestos a internet (parcial) • Protección contra malware supervisada (parcial) • Prueba de restauración (no implementado)
Fraude por suplantación de correo (pago a cuenta falsa)	ALTA	\$150,000 MXN · \$300,000 MXN · \$600,000 MXN	• Verificación en dos pasos en correo y nube (no implementado) • Capacitación por rol (TI y pagos) (iniciado) • Seguridad del correo electrónico (parcial)
Vulneración de datos personales	ALTA	Implica obligaciones de aviso a los titulares y posibles sanciones conforme a la LFPDPPP; el monto depende del caso y debe evaluarse con asesoría jurídica.	• Inventario de datos sensibles (parcial) • Mínimo privilegio y cuentas de administrador separadas (parcial) • Cifrado en tránsito (parcial) • Obligaciones legales y contractuales (iniciado)

Supuestos: Ingreso en riesgo = ingreso mensual ÷ 30 × días de interrupción. Los días de interrupción y el costo de respuesta (atención técnica, legal y de comunicación) son supuestos de Proventum por tamaño de empresa, a calibrar; no son estadísticas de terceros. Los montos son ingreso en riesgo, no utilidad perdida. Ingreso mensual declarado: \$2,500,000 MXN. Costo de respuesta supuesto para su tamaño: \$60,000 MXN · \$150,000 MXN · \$400,000 MXN. Fraude por correo: 0.5, 1 y 2 veces el monto de transferencia declarado.

Riesgo de proveedores de tecnología

Proveedor	Categoría	Nivel	Requisitos mínimos a exigir
Proveedor de soporte (ejemplo)	Soporte de TI con acceso remoto Acceso privilegiado a sistemas	CRÍTICO	• Anexo de seguridad y protección de datos en el contrato • MFA obligatorio para sus accesos • Aviso de incidentes en un plazo definido • Evidencia de controles (certificación o cuestionario anual) • Devolución o borrado de datos al terminar Proveedor crítico y la empresa indicó que sus contratos casi no tienen cláusulas de seguridad.
ERP en la nube (ejemplo)	ERP / Contabilidad Datos financieros y operativos	CRÍTICO	• Anexo de seguridad y protección de datos en el contrato • MFA obligatorio para sus accesos • Aviso de incidentes en un plazo definido • Evidencia de controles (certificación o cuestionario anual) • Devolución o borrado de datos al terminar Proveedor crítico y la empresa indicó que sus contratos casi no tienen cláusulas de seguridad.

Equivalencias indicativas

NIST CSF 2.0: este diagnóstico evaluó prácticas relacionadas con 54 de las 106 subcategorías del marco.

Datos personales (LFPDPPP): 11 de 26 prácticas relacionadas con el deber de seguridad están mayoritaria o completamente implementadas (42%).

Pendientes: GV-02 Política de seguridad aprobada; GV-03 Obligaciones legales y contractuales; GV-06 Seguridad al contratar y al dar de baja; GV-08 Cláusulas de seguridad con proveedores; ID-03 Inventario de datos sensibles; PR-01 Verificación en dos pasos en correo y nube; PR-03 Cuentas personales e intransferibles; PR-04 Mínimo privilegio y cuentas de administrador separadas; PR-07 Capacitación anual en seguridad; PR-11 Cifrado en tránsito; PR-12 Respallos automáticos de información crítica; PR-23 Registros de actividad; PR-25 Trabajo remoto y equipos personales; RS-01 Plan de respuesta a incidentes; RC-01 Prueba de restauración.

ISO/IEC 27001:2022 — referencias relacionadas

5.1 Parcial	5.2 Atendido	5.7 Parcial	5.9 Atendido
5.12 Parcial	5.14 Parcial	5.15 Parcial	5.16 Brecha
5.17 Atendido	5.18 Brecha	5.19 Atendido	5.20 Brecha
5.24 Parcial	5.26 Parcial	5.29 Brecha	5.30 Brecha
5.31 Brecha	5.34 Parcial	6.1 Brecha	6.2 Brecha
6.3 Brecha	6.5 Brecha	6.7 Brecha	6.8 Atendido
7.2 Atendido	7.14 Atendido	8.1 Parcial	8.2 Parcial
8.5 Brecha	8.7 Parcial	8.8 Parcial	8.9 Atendido
8.13 Brecha	8.15 Brecha	8.16 Parcial	8.20 Parcial
8.21 Atendido	8.22 Brecha	8.24 Atendido	Cláusula 7.1 Parcial
Cláusula 9.3 Parcial	Cláusulas 6.1.2 y 8.2 Atendido		

Equivalencias indicativas a partir de respuestas declaradas. No constituyen una auditoría ni una opinión jurídica.

Qué indica cada métrica

Gobernar (GOVERN)	51 de 100. Prácticas parciales; hay brechas por cerrar.
Identificar (IDENTIFY)	63 de 100. Prácticas parciales; hay brechas por cerrar.
Proteger (PROTECT)	50 de 100. Prácticas parciales; hay brechas por cerrar.
Detectar (DETECT)	64 de 100. Prácticas parciales; hay brechas por cerrar.
Responder (RESPOND)	56 de 100. Prácticas parciales; hay brechas por cerrar.
Recuperar (RECOVER)	28 de 100. Pocas prácticas implementadas; es una prioridad.
Controles llave adecuados	2 de 7 controles llave están mayoritaria o completamente implementados.

• SECCIÓN 06

Análisis e interpretación

Qué significan los resultados para la empresa evaluada.

El score de 39 de 100 resume qué tanto de las prácticas evaluadas tiene implementadas la empresa; el nivel Básico corresponde a la escala propia de NexCyber, que va de Inicial a Optimizado. No es un dictamen de seguridad: describe prácticas declaradas por la empresa.

Los controles llave son las prácticas que más reducen la probabilidad y el impacto de un ataque. Mientras alguno esté ausente o apenas iniciado, la exposición sigue siendo alta aunque otras prácticas estén en orden; por eso el score general se limitó a 39 de 100.

Se identificaron 29 brechas. El plan las agrupa en paquetes que conviene hacer juntos y en orden (por ejemplo, primero respaldos y después la prueba de restauración), empezando por los controles llave, y sube de prioridad lo que se relaciona con vulnerabilidades explotadas en sus productos, escenarios de pérdida más probables o proveedores con alerta. Cada paquete trae una meta verificable, un primer paso para esta semana y su efecto estimado en el score.

Alertas

Controles llave

Sin el tope por controles llave el score habría sido 52 de 100.

Vulnerabilidades

2 vulnerabilidades explotadas en sus productos tienen uso conocido en campañas de ransomware; verifique con su proveedor si su versión está afectada.

Respuestas a confirmar

Algunas respuestas parecen no coincidir entre sí. Puede ser correcto, pero conviene confirmarlas con su responsable de TI, porque cambian el orden del plan:

- PR-13 Copia de respaldo aislada o inmutable se declaró mayoritario, pero PR-12 Respaldos automáticos de información crítica quedó en no implementado. Conviene confirmar ambas respuestas: una copia aislada suele depender de que existan respaldos automáticos.
- ID-06 Búsqueda de vulnerabilidades se declaró completo y revisado, y el catálogo CISA KEV muestra 3 vulnerabilidades explotadas en productos declarados, 2 con uso en ransomware. Conviene confirmar que la revisión cubre esos equipos y su versión.

SECCIÓN 07

Recomendaciones

Acciones sugeridas, ligadas a los hallazgos de este reporte.

Primeros 7 días

Lo que conviene hacer esta semana, antes de entrar a los paquetes:

1. Liste los sistemas críticos (sistema administrativo, correo, archivos y nube), confirme cuáles tienen respaldo automático y configure el primero que falte.
2. Active la verificación en dos pasos en las cuentas de dirección, finanzas y administradores del correo y la nube, y fije la fecha para hacerla obligatoria a todos.
3. Confirme con su proveedor la versión que usa de PHP y ConnectWise ScreenConnect y si le aplica CVE-2024-4577 y CVE-2024-1709; si aplica, corrija o mitigue en 7 días o menos.
4. Revise con su responsable de TI las respuestas que parecen no coincidir (PR-13, PR-12, ID-06).

1

Paquete de recuperación, en este orden: 1) implementar los respaldos automáticos de información crítica (PR-12, no implementado); 2) implementar la prueba de restauración con tiempo medido (RC-01, no implementado); 3) formalizar el plan de recuperación del negocio (RC-03, iniciado).

PRIORIDAD ALTA

INMEDIATO

Meta	Respaldos automáticos de todos los sistemas críticos, con frecuencia alineada al objetivo de pérdida máxima de datos. Prueba semestral exitosa de los sistemas críticos, con tiempo medido contra el objetivo. Plan aprobado y revisado en los últimos 12 meses.
Primer paso	Esta semana liste los sistemas críticos (sistema administrativo, correo, archivos y nube), confirme cuáles tienen respaldo automático y configure el primero que falte.
Cómo medirlo	Evidencia: Reporte de la herramienta de respaldo; bitácora de ejecuciones; informe de la prueba de restauración; plan de recuperación o continuidad.
Efecto estimado	Score estimado de 39 a 59 si llega a nivel Mayoritario; atiende 2 controles llave; sube el tope de 39 a 59.
Hallazgo relacionado	PR-12 no implementado, RC-01 no implementado, RC-03 iniciado; sube de prioridad por escenario de ransomware con probabilidad Media (rango medio \$1,317,000 MXN)

2

Paquete de acceso seguro, en este orden: 1) implementar la verificación en dos pasos en correo y nube (PR-01, no implementado); 2) completar el mínimo privilegio y las cuentas de administrador separadas (PR-04, parcial); 3) formalizar las cuentas personales e intransferibles (PR-03, iniciado).

PRIORIDAD ALTA
INMEDIATO

Meta	100 % de los usuarios con MFA obligatorio, sin excepciones permanentes; métodos resistentes a phishing para administradores. Ningún usuario de uso diario con permisos de administrador; cuentas administrativas separadas y registradas. Sin cuentas compartidas para personas; bajas aplicadas en menos de 24 horas.
Primer paso	Esta semana active la verificación en dos pasos en las cuentas de dirección, finanzas y administradores del correo y la nube, y fije la fecha para hacerla obligatoria a todos.
Cómo medirlo	Evidencia: Captura de la consola que muestre el MFA obligatorio; lista de cuentas con privilegios; lista de cuentas; registro de bajas.
Efecto estimado	Score sin tope de 52 a 54; el general sigue en 39 mientras falten otros controles llave; atiende un control llave.
Hallazgo relacionado	PR-01 no implementado, PR-04 parcial, PR-03 iniciado; sube de prioridad por escenario de fraude por correo con probabilidad Alta (rango medio \$300,000 MXN)

3

Paquete de parcheo y actualizaciones, en este orden: 1) completar el parcheo urgente de equipos expuestos a internet (PR-15, parcial); 2) formalizar las actualizaciones de sistemas y aplicaciones (PR-14, iniciado).

PRIORIDAD ALTA
INMEDIATO

Meta	Fallas explotadas activamente corregidas o mitigadas en 7 días o menos. Al menos el 95 % de los equipos al día; actualizaciones críticas en 30 días o menos.
Primer paso	Esta semana confirme con su proveedor la versión que usa de PHP y ConnectWise ScreenConnect y si le aplica CVE-2024-4577 y CVE-2024-1709; si aplica, corrija o mitigue en 7 días o menos.
Cómo medirlo	Evidencia: Registro de actualizaciones de equipos perimetrales; reporte de la consola de actualizaciones.
Efecto estimado	Score sin tope de 52 a 53; el general sigue en 39 mientras falten otros controles llave; menos exposición a fallas ya explotadas.
Hallazgo relacionado	PR-15 parcial, PR-14 iniciado; sube de prioridad por 3 vulnerabilidades explotadas en productos declarados, 2 con uso en ransomware

4

Paquete contra fraude por correo, en este orden: 1) formalizar la capacitación por rol y la doble verificación de pagos (PR-09, iniciado); 2) completar la seguridad del correo con SPF, DKIM y DMARC (PR-22, parcial).

PRIORIDAD MEDIA
CORTO PLAZO

Meta	Capacitación anual por rol y regla de doble verificación de pagos aplicada. Filtro activo y DMARC en modo de cuarentena o rechazo.
Primer paso	Esta semana comunique por escrito a finanzas la regla: todo cambio de cuenta bancaria de un proveedor se confirma por teléfono a un número ya registrado.
Cómo medirlo	Evidencia: Constancias; procedimiento de verificación de pagos; configuración DNS del dominio; consola del filtro.
Efecto estimado	Sin cambio visible en el score; fraude por correo: probabilidad de Alta a Media.
Hallazgo relacionado	PR-09 iniciado, PR-22 parcial; sube de prioridad por escenario de fraude por correo con probabilidad Alta (rango medio \$300,000 MXN)

5

Paquete de detección, en este orden: 1) completar la protección contra malware supervisada (PR-18, parcial); 2) completar la atención diaria de alertas (DE-01, parcial); 3) implementar los registros de actividad (PR-23, no implementado).

PRIORIDAD MEDIA

CORTO PLAZO

Meta	100 % de cobertura con consola central; de preferencia una solución con detección por comportamiento (EDR). Responsable asignado (interno o proveedor) con revisión diaria y registro de atención. Registros activados en todos los sistemas críticos, conservados 90 días o más.
Primer paso	Esta semana compare el inventario de equipos contra el reporte de la consola de protección y anote los equipos que faltan.
Cómo medirlo	Evidencia: Reporte de cobertura de la consola; registro de alertas atendidas; contrato de monitoreo; configuración de registros; muestra de registros.
Efecto estimado	Score sin tope de 52 a 54; el general sigue en 39 mientras falten otros controles llave.
Hallazgo relacionado	PR-18 parcial, DE-01 parcial, PR-23 no implementado

El efecto es una simulación con la misma fórmula del diagnóstico: las prácticas del paquete pasan a nivel 3 (Mayoritario) y las demás respuestas no cambian. El plan completo, con todas las brechas por plazo, está en la sección de resultados.

Las recomendaciones son sugerencias de apoyo analítico basadas en los datos de este reporte. La decisión final corresponde a la empresa y, cuando aplique, a sus asesores profesionales.

SECCIÓN 08

Metodología, fuentes y limitaciones

Cómo se generó este reporte y qué debes considerar al usarlo.

Metodología

NexCyber evalúa prácticas concretas del **Catálogo de Salvaguardas Proventum**, redactado por Proventum y organizado según las seis funciones de **NIST CSF 2.0**. Cada práctica se responde de 0 (no implementado) a 4 (completo y revisado); “no sé” cuenta como 0.

El score de cada práctica es la respuesta entre 4 por 100; el de cada función, el promedio ponderado por el peso de sus prácticas (1 a 3); el general pondera las funciones (Gobernar 15%, Identificar 15%, Proteger 30%, Detectar 15%, Responder 10%, Recuperar 15%). **Tope:** con un control llave en 0 o 1 el score general no pasa de 59; con dos o más, no pasa de 39.

Las brechas son las prácticas con respuesta de 2 o menos, priorizadas por peso, avance y si son control llave, y suben de prioridad si se relacionan con vulnerabilidades explotadas en los productos declarados, con un escenario de pérdida de probabilidad alta o media o con proveedores críticos sin cláusulas de seguridad. Las recomendaciones agrupan las brechas en paquetes que conviene hacer juntos y en orden; su meta y su evidencia vienen del catálogo, y el efecto en el score se recalcula con la misma fórmula, suponiendo que las prácticas del paquete llegan a nivel 3 (Mayoritario). En Integral, las vulnerabilidades se buscan por fabricante y producto en el catálogo CISA KEV (últimos 24 meses) y se complementan con FIRST EPSS.

Fuentes de información

Fuente	Uso en este reporte	Vigencia / consulta
Respuestas declaradas por la empresa	Base de todo el cálculo	15/10/2026 17:58
Catálogo de Salvaguardas Proventum v0.1	Prácticas evaluadas, mapeadas a NIST CSF 2.0 (CSWP 29) e ISO/IEC 27001:2022	Versión vigente
CISA Known Exploited Vulnerabilities (KEV)	Vulnerabilidades explotadas por producto	demostración
FIRST EPSS	Probabilidad de explotación a 30 días	Caché de hasta 24 horas

Limitaciones

- Es un diagnóstico de madurez basado en respuestas declaradas: no es una auditoría, no es una prueba de penetración y no certifica a la empresa en ninguna norma.
- La escala de madurez (Inicial a Optimizado) es propia de NexCyber y no equivale a los Tiers de NIST CSF.
- Las equivalencias con ISO/IEC 27001 y la LFPDPPP son indicativas y no constituyen una opinión jurídica.
- Los escenarios de pérdida usan supuestos de Proventum por tamaño de empresa (días de interrupción y costo de respuesta); son rangos para planear, no pronósticos.
- Las cifras de entrada las declara el usuario y no se verifican contra documentos originales.

Privacidad

Este reporte es confidencial y pertenece al titular de la cuenta. Las respuestas se usan para generar este diagnóstico y se conservan ligadas al folio para prellenar el siguiente; no se venden, no se comparten con fines comerciales y no se usan para entrenar modelos de IA. Para redactar los textos, las cifras calculadas pueden enviarse a un proveedor de IA (Anthropic, API de Claude) únicamente con ese fin. El reporte se envía al correo del titular y se guarda en su cuenta solo si lo autorizó.

Aviso importante

Herramienta de **apoyo analítico** generada con procesos automatizados e inteligencia artificial a partir de fuentes públicas u oficiales, que pueden tener errores u omisiones o estar desactualizadas. **No es asesoría financiera, fiscal, legal, contable, aduanal ni de inversión**, ni una garantía o dictamen. Cada decisión es responsabilidad de quien la toma; válidala con las fuentes oficiales y con un profesional.