

● 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

Básico

PRÁCTICAS EVALUADAS

20

NIVEL DE MADUREZ

55/100 · EN DESARROLLO

Prácticas parciales; hay brechas importantes por atender.

55/100

Score NexCyber

3 de 7

Controles llave adecuados

12

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-BASICO

FECHA DE GENERACIÓN

15/10/2026 12:00

MOTOR

NexCyber · NexIntelía

• SECCIÓN 02

Resumen ejecutivo

Lo esencial del resultado, en lenguaje claro.

55/100

Score NexCyber

En desarrollo

Nivel de madurez

3 de 7

Controles llave adecuados

12

Brechas identificadas

La empresa evaluada obtiene 55 de 100 en el diagnóstico NexCyber, nivel de madurez En desarrollo. Las acciones prioritarias se concentran en las prácticas con menor avance.

Hallazgos clave

- 01** La función más sólida es Detectar con 75 de 100 y la más débil es Responder con 25 de 100.
- 02** Controles llave ausentes o apenas iniciados: verificación en dos pasos en correo y nube.
- 03** Qué atender primero (0–30 días): Paquete de acceso seguro. Score estimado de 55 a 61 si llega a nivel Mayoritario; atiende un control llave.

PDF de ejemplo

Empresa y respuestas ficticias, para mostrar el formato del reporte.

• 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	Básico
Prácticas respondidas	20
Respondidas con "no sé"	0
Fecha del diagnóstico	15/10/2026 17:58

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%	2	65	
Identificar (IDENTIFY)	15%	3	54	
Proteger (PROTECT)	30%	11	47	
Detectar (DETECT)	15%	1	75	
Responder (RESPOND)	10%	1	25	
Recuperar (RECOVER)	15%	2	63	

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.

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	Mayoritario	ADECUADO
PR-13 Copia de respaldo aislada o inmutable	Parcial	REFORZAR
PR-15 Parcheo urgente de equipos expuestos a internet	Completo y revisado	ADECUADO
PR-18 Protección contra malware supervisada	Parcial	REFORZAR
RC-01 Prueba de restauración	Parcial	REFORZAR

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-21 Sin servicios administrativos expuestos	Proteger	No implementado	CRÍTICA
3	RS-01 Plan de respuesta a incidentes	Responder	Iniciado	ALTA
4	ID-01 Inventario de equipos	Identificar	Iniciado	ALTA
5	PR-04 Mínimo privilegio y cuentas de administrador separadas	Proteger	Iniciado	ALTA

• SECCIÓN 05

Acciones prioritarias

Indicadores adicionales y qué indica cada uno.

Acciones prioritarias

#	Acción sugerida	Plazo sugerido	Esfuerzo
1	Verificación en dos pasos en correo y nube Activar el MFA obligatorio en correo y nube para todos los usuarios.	0–30 días	Bajo
2	Sin servicios administrativos expuestos Cerrar los servicios administrativos expuestos y publicarlos solo detrás de una VPN con MFA.	0–30 días	Bajo
3	Plan de respuesta a incidentes Redactar un plan breve con guías para ransomware, fraude por correo y robo de cuenta.	0–30 días	Bajo
4	Inventario de equipos Implementar un inventario (de preferencia automático) y asignar un responsable a cada equipo.	0–30 días	Bajo
5	Mínimo privilegio y cuentas de administrador separadas Retirar los permisos de administrador del uso diario y crear cuentas administrativas separadas.	0–30 días	Bajo
6	Actualizaciones de sistemas y aplicaciones Activar las actualizaciones automáticas y revisar cada mes los equipos rezagados.	0–30 días	Bajo
7	Copia de respaldo aislada o inmutable Agregar una copia desconectada o inmutable (por ejemplo, almacenamiento en la nube con bloqueo de borrado).	31–90 días	Medio
8	Prueba de restauración Programar una prueba de restauración cada semestre y documentar el tiempo.	31–90 días	Bajo
9	Protección contra malware supervisada Desplegar una solución administrada centralmente (de preferencia EDR) en todos los equipos.	31–90 días	Medio
10	Evaluación periódica de riesgos Realizar una evaluación anual (puede ser NexCyber) y mantener un registro de riesgos con responsables.	91–180 días	Bajo

Ordenadas por plazo y, dentro de cada plazo, por impacto. El esfuerzo es relativo (Bajo, Medio o Alto).

Qué indica cada métrica

Gobernar (GOVERN)	65 de 100. Prácticas parciales; hay brechas por cerrar.
Identificar (IDENTIFY)	54 de 100. Prácticas parciales; hay brechas por cerrar.
Proteger (PROTECT)	47 de 100. Pocas prácticas implementadas; es una prioridad.
Detectar (DETECT)	75 de 100. Prácticas mayoritaria o completamente implementadas.
Responder (RESPOND)	25 de 100. Pocas prácticas implementadas; es una prioridad.
Recuperar (RECOVER)	63 de 100. Prácticas parciales; hay brechas por cerrar.
Controles llave adecuados	3 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 55 de 100 resume qué tanto de las prácticas evaluadas tiene implementadas la empresa; el nivel En desarrollo 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; si el score subiera, quedaría limitado a 59 hasta atenderlos.

Se identificaron 12 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. Cada paquete trae una meta verificable, un primer paso para esta semana y su efecto estimado en el score.

No se identificaron alertas con los datos de este reporte.

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-15 Parcheo urgente de equipos expuestos a internet se declaró completo y revisado, pero PR-14 Actualizaciones de sistemas y aplicaciones quedó en iniciado. Conviene confirmar ambas respuestas: el parcheo urgente suele apoyarse en un proceso general de actualizaciones.

¿Quiere el diagnóstico completo?

NexCyber Integral evalúa todas las prácticas esenciales del catálogo y agrega un plan de acción completo por plazos, vulnerabilidades explotadas en sus productos, escenarios de pérdida en pesos, riesgo de proveedores y equivalencias con ISO/IEC 27001 y la LFPDPPP. Sus respuestas del Básico se precargan.

• 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. 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.
2. Active las actualizaciones automáticas en los equipos que lo permitan y obtenga la lista de equipos rezagados.
3. Arme el directorio de contactos de emergencia (TI, proveedor de soporte, aseguradora y asesoría jurídica) y la primera guía: qué hacer ante ransomware.
4. Revise con su responsable de TI las respuestas que parecen no coincidir (PR-15, PR-14).

1

Paquete de acceso seguro, en este orden: 1) implementar la verificación en dos pasos en correo y nube (PR-01, no implementado); 2) implementar el cierre de servicios administrativos expuestos (PR-21, no implementado); 3) formalizar el mínimo privilegio y las cuentas de administrador separadas (PR-04, iniciado).

PRIORIDAD ALTA

INMEDIATO

Meta	100 % de los usuarios con MFA obligatorio, sin excepciones permanentes; métodos resistentes a phishing para administradores. Ningún servicio administrativo expuesto sin VPN o acceso con MFA. Ningún usuario de uso diario con permisos de administrador; cuentas administrativas separadas y registradas.
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; revisión externa de puertos; configuración del firewall; lista de cuentas con privilegios.
Efecto estimado	Score estimado de 55 a 61 si llega a nivel Mayoritario; atiende un control llave.
Hallazgo relacionado	PR-01 no implementado, PR-21 no implementado, PR-04 iniciado

2

Paquete de parcheo y actualizaciones, en este orden: 1) formalizar las actualizaciones de sistemas y aplicaciones (PR-14, iniciado); 2) completar la búsqueda mensual de vulnerabilidades (ID-06, parcial).

PRIORIDAD MEDIA

INMEDIATO

Meta	Al menos el 95 % de los equipos al día; actualizaciones críticas en 30 días o menos. Revisión mensual automatizada, hallazgos registrados y atendidos según su gravedad.
Primer paso	Esta semana active las actualizaciones automáticas en los equipos que lo permitan y obtenga la lista de equipos rezagados.
Cómo medirlo	Evidencia: Reporte de la consola de actualizaciones; reportes de escaneo; registro de hallazgos.
Efecto estimado	Score estimado de 55 a 57 si llega a nivel Mayoritario.
Hallazgo relacionado	PR-14 iniciado, ID-06 parcial

3

Formalizar lo que ya se inició y llevarlo a toda la empresa: redactar un plan breve con guías para ransomware, fraude por correo y robo de cuenta.

PRIORIDAD MEDIA

INMEDIATO

Meta	Plan aprobado, revisado en los últimos 12 meses y conocido por los responsables.
Primer paso	Esta semana arme el directorio de contactos de emergencia (TI, proveedor de soporte, aseguradora y asesoría jurídica) y la primera guía: qué hacer ante ransomware.
Cómo medirlo	Evidencia: Plan de respuesta; directorio de contactos.
Efecto estimado	Score estimado de 55 a 59 si llega a nivel Mayoritario.
Hallazgo relacionado	RS-01 Plan de respuesta a incidentes: iniciado

4

Formalizar lo que ya se inició y llevarlo a toda la empresa: implementar un inventario (de preferencia automático) y asignar un responsable a cada equipo.

PRIORIDAD MEDIA

INMEDIATO

Meta	Inventario con al menos el 95 % de los equipos, actualizado como mínimo cada trimestre (idealmente de forma automática).
Primer paso	Esta semana exporte una primera lista de equipos (de la red o de la consola de protección) y asigne un responsable a cada uno.
Cómo medirlo	Evidencia: Exportación del inventario; herramienta de inventario.
Efecto estimado	Score estimado de 55 a 58 si llega a nivel Mayoritario.
Hallazgo relacionado	ID-01 Inventario de equipos: iniciado

5

Paquete de recuperación, en este orden: 1) completar la copia de respaldo aislada o inmutable (PR-13, parcial); 2) completar la prueba de restauración con tiempo medido (RC-01, parcial).

PRIORIDAD MEDIA

CORTO PLAZO

Meta	Copia aislada o inmutable verificada para todos los sistemas críticos. Prueba semestral exitosa de los sistemas críticos, con tiempo medido contra el objetivo.
Primer paso	Esta semana verifique qué sistemas críticos aún no tienen copia aislada o inmutable y que la copia existente no pueda borrarse con las cuentas de uso diario.
Cómo medirlo	Evidencia: Configuración de la copia aislada o inmutable; informe de la prueba de restauración.
Efecto estimado	Score estimado de 55 a 58 si llega a nivel Mayoritario.
Hallazgo relacionado	PR-13 parcial, RC-01 parcial

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. La tabla de acciones prioritarias de la sección de resultados muestra las 10 primeras brechas por plazo.

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. 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).

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

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.
- 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.