INFORME DE EVALUACIÓN

Ciberseguridad Empresarial

No especificado

No especificado · No especificado

Preparado para: No especificado · No especificado
Fecha: 19 de enero de 2026

Evaluación basada en el Framework NIST Cybersecurity
Powered by Nuvo Corp · www.nuvo.pe

Resumen Ejecutivo

No especificado cuenta con controles básicos, con oportunidades significativas de mejora. Fortalezas: respaldos en cambios críticos; pruebas de restauración. Áreas de mejora: sin capacitación en seguridad; sin monitoreo de credenciales comprometidas.

Nivel de Madurez General

Básico

Controles básicos implementados pero sin formalización. Existen oportunidades significativas de mejora.

Nivel 2 de 5

Puntuación por Función NIST

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
2/5	2/5	2/5	1/5	3/5

Perfil de la Empresa

EMPRESA No especificado	INDUSTRIA No especificado	PAÍS No especificado
TAMAÑO No especificado	INFRAESTRUCTURA No especificado	CLOUD No especificado

Hallazgos Principales

⚠️ Brechas Identificadas

- ! Sin capacitación en seguridad
- ! Sin monitoreo de credenciales comprometidas
- ! Sin plan de respuesta a incidentes

✅ Fortalezas Detectadas

- ✓ Respaldos en cambios críticos
- ✓ Pruebas de restauración
- ✓ Permisos y roles implementados

Soluciones Recomendadas

1. **BullPhish ID**
   Entrenamiento y simulaciones de phishing.

2. **Dark Web ID**
   Monitoreo de credenciales comprometidas en la dark web.

3. **Managed SOC**
   Solución recomendada basada en el assessment.

Evaluación Detallada por Función NIST

IDENTIFICAR

Gestión de activos, riesgos y gobernanza

2/5
Puntuación

Hallazgos:

Inventario parcial de activos. Evaluación de riesgos informal.

Recomendaciones:

Implementar gestión de activos y evaluación de vulnerabilidades.

PROTEGER

Controles de acceso y seguridad de datos

2/5
Puntuación

Hallazgos:

Áreas de mejora: Sin capacitación en seguridad.

Recomendaciones:

Fortalecer MFA, programa de concientización y políticas de acceso.

DETECTAR

Monitoreo continuo y detección de amenazas

2/5
Puntuación

Hallazgos:

Áreas de mejora: Sin monitoreo de credenciales comprometidas.

Recomendaciones:

Implementar monitoreo continuo y considerar SOC gestionado.

RESPONDER

Planificación y gestión de incidentes

1/5

Puntuación

Hallazgos:

Áreas de mejora: Sin plan de respuesta a incidentes.

Recomendaciones:

Documentar plan de respuesta y realizar simulacros.

RECUPERAR

Respaldo, continuidad y resiliencia

3/5

Puntuación

Hallazgos:

Fortalezas: Respaldos en cambios críticos.

Recomendaciones:

Implementar respaldo híbrido, definir RTO/RPO y probar recuperación.

Plan de Acción Recomendado

1. **Corto Plazo (0-30 días)**
   Implementar monitoreo de activos críticos y alertas básicas.

2. **Mediano Plazo (30-90 días)**
   Implementar BullPhish ID y Dark Web ID. Establecer métricas de seguridad.

3. **Largo Plazo (90+ días)**
   Establecer programa integral de seguridad. Considerar certificación ISO 27001.

¿Listo para fortalecer tu seguridad?

Nuestro equipo de especialistas está disponible para ayudarte a implementar estas recomendaciones.

WEB
www.nuvo.pe

EMAIL
contacto@nuvo.pe

TELÉFONO
+51 1 234 5678