UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA

FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

MAESTRÍA EN ANÁLISIS FORENSE INFORMÁTICO

TAREA NO. 7

GAP ANÁLISIS DE CUMPLIMIENTO NIST CSF 2.0 Y AUDITORÍA DE FIREWALL FORTIGATE 2000E

Autor:

Brandon Eduardo Godinez Suret

2693-18-7504

bgodinezs1@miumg.edu.gt

Profesor
MSc. Ing. Déner Medrano

Curso
Auditoría Informática – 4 – 2,025

Guatemala 22 de noviembre, 2025

Rúbrica, calificación y firma electrónica

Rúbrica	
100%	Excelente
80%	Bueno
60%	Regular
40%	Limitado
20%	Debe mejorar bastante
0%	Inaceptable

Contenido

Introducción

La ciberseguridad se ha convertido en un pilar fundamental para la continuidad y el éxito de las organizaciones modernas, especialmente aquellas que buscan expandir sus operaciones y establecer alianzas internacionales. En este contexto, la presente tarea aborda dos procesos clave: el GAP análisis de cumplimiento basado en el marco NIST Cybersecurity Framework (CSF) 2.0 y la auditoría técnica del firewall Fortigate 2000E.

El objetivo principal es evaluar el nivel de madurez en ciberseguridad de la organización, identificar brechas y riesgos críticos, y proponer acciones concretas para fortalecer la protección de los activos tecnológicos. Para ello, se empleó la herramienta CSET de CISA, permitiendo una autoevaluación estructurada y alineada con estándares internacionales. Posteriormente, se realizó una auditoría externa sobre el firewall Fortigate 2000E, revisando configuraciones, políticas y controles aplicados, con base en los marcos ISO 27001 y NIST SP 800-41.

Este trabajo integra el análisis de cumplimiento, la documentación de hallazgos técnicos, el análisis de riesgos y la elaboración de un plan de remediación, todo ello bajo un enfoque profesional y ético, respaldado por un acuerdo de confidencialidad. Los resultados obtenidos servirán como base para la toma de decisiones estratégicas y la preparación ante auditorías externas, contribuyendo al fortalecimiento de la postura de seguridad de la organización.

Capítulo 1

GAP Análisis según NIST CSF 2.0

1.1 Objetivos del Assessment

1.1.1 Objetivo General

Realizar un GAP Análisis basado en el marco de trabajo NIST Cybersecurity Framework (CSF) 2.0, utilizando la herramienta CSET de CISA, con el propósito de evaluar el nivel actual de madurez en ciberseguridad de la organización y determinar el grado de cumplimiento requerido para concretar la alianza estratégica con una empresa de los Estados Unidos.

1.1.2 Objetivos Específicos

A. **Identificar el estado actual de la postura de ciberseguridad**, evaluando las cinco funciones del NIST CSF 2.0: *Identify, Protect, Detect, Respond* y *Recover*.
B. **Detectar brechas, debilidades y controles insuficientes** dentro de la infraestructura tecnológica, considerando entornos IT, OT, IoT y sistemas industriales descritos en el contexto empresarial.
C. **Analizar los niveles de riesgo asociados a cada brecha**, evaluando impacto, probabilidad y urgencia de implementación de mejoras.
D. **Determinar el grado de cumplimiento por categoría del NIST CSF 2.0**, con base en los resultados generados por CSET y la evidencia recopilada.
E. **Establecer un conjunto de prioridades y acciones recomendadas**, que sirvan como plan de fortalecimiento de seguridad previo a la auditoría formal que realizará un tercero internacional.

1.2 Alcance de la Evaluación

El alcance del presente assessment abarca la revisión integral de la postura de ciberseguridad de la organización, considerando los activos, procesos y entornos tecnológicos descritos en el contexto institucional. La evaluación se realizó utilizando el marco NIST Cybersecurity Framework (CSF) 2.0 mediante la herramienta CSET de CISA, e incluye tanto componentes de TI corporativa como elementos de tecnología operacional (OT).

En particular, el alcance cubre los siguientes elementos:

- **Infraestructura de TI**: servidores corporativos, ERP **SAP Hana**, integraciones con proveedores externos, redes internas y equipos de usuario final.
- **Infraestructura industrial y OT**: sistemas **SCADA**, redes industriales segregadas por VLANs, sistemas de control industrial y equipos legacy presentes en plantas de producción.
- **Dispositivos IoT** utilizados en procesos de monitoreo y automatización dentro de las operaciones de manufactura.
- **Controles de seguridad existentes**, incluyendo el firewall **Checkpoint con IPS**, antivirus **Microsoft Defender**, y redes inalámbricas empresariales basadas en Access Points Ubiquiti.
- **Procesos de gestión de seguridad**, tales como monitoreo, respuesta a incidentes, continuidad del negocio, y recuperación ante desastres, los cuales actualmente presentan limitaciones relevantes (ausencia de SOC, DRP y BCP).

Quedan fuera del alcance actividades de explotación técnica, pruebas intrusivas o auditorías de código fuente, dado que el objetivo principal es evaluar el nivel de madurez frente al NIST CSF 2.0 y determinar las brechas existentes antes de la llegada del auditor extranjero.

1.3 Marco de Trabajo: NIST CSF 2.0

El assessment se basa en el **NIST Cybersecurity Framework (CSF) 2.0**, un estándar internacional utilizado para evaluar y fortalecer la postura de ciberseguridad de una organización. El marco se estructura en cinco funciones principales:

- **Identify (ID):** Comprender los activos, riesgos y entorno operativo.
- **Protect (PR):** Implementar controles que reduzcan la probabilidad de incidentes.
- **Detect (DE):** Identificar eventos anómalos o actividades maliciosas.
- **Respond (RS):** Contener y mitigar incidentes de seguridad.
- **Recover (RC):** Restaurar servicios y operaciones después de un incidente.

Estas funciones permiten realizar un análisis organizado y medir el nivel de madurez de la organización, identificando brechas y áreas prioritarias de mejora.

1.4 Infraestructura Evaluada

La evaluación se realizó tomando como referencia la infraestructura tecnológica descrita en el caso práctico, considerando los componentes que impactan directamente en la postura de ciberseguridad de la organización. La infraestructura evaluada incluye:

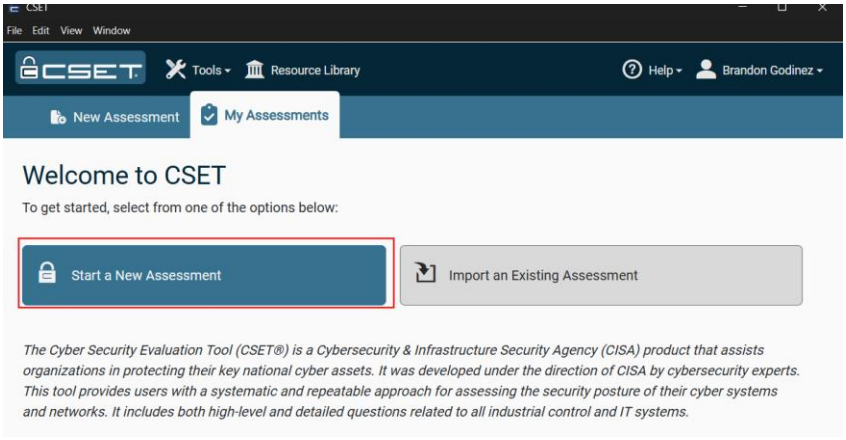
- **ERP SAP Hana** utilizado para la gestión central de operaciones.
- **Sistemas SCADA** implementados en las plantas de producción.
- **Red OT** segmentada mediante VLANs para control industrial.
- **Infraestructura legacy** presente en entornos operativos.
- **Sistemas de control industrial** críticos para procesos de manufactura.
- **Dispositivos IoT** utilizados para monitoreo y supervisión.
- **Integraciones con proveedores externos**, esenciales para la cadena de suministro.
- **Firewall Checkpoint con IPS** habilitado para la protección perimetral.
- **Antivirus Microsoft Defender** desplegado en endpoints corporativos.
- **Redes inalámbricas empresariales** basadas en Access Points Ubiquiti.

Esta infraestructura sirve como base para identificar brechas de seguridad, evaluar controles existentes y determinar el nivel de cumplimiento frente al NIST CSF 2.0.

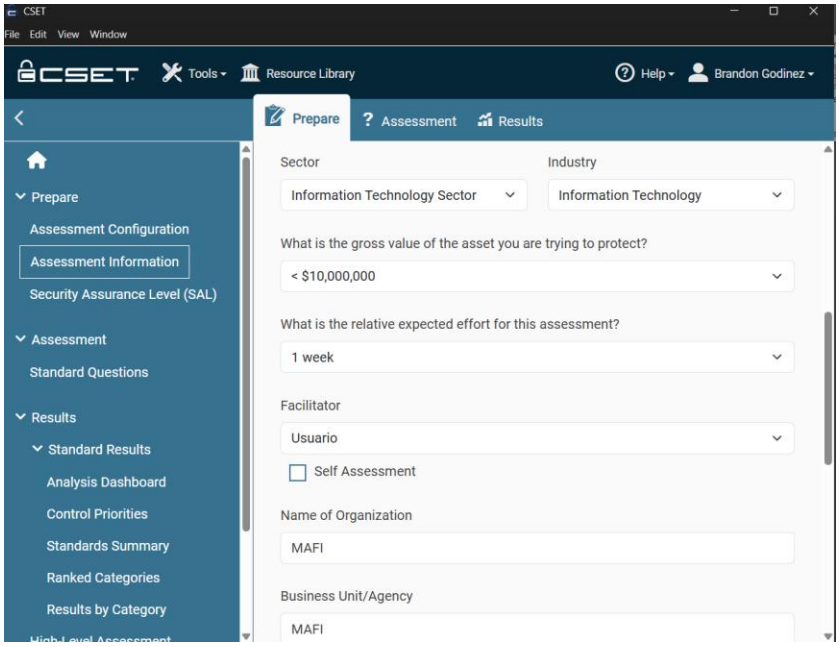
1.5 Procedimiento realizado con CSET

El assessment se llevó a cabo utilizando la herramienta **CSET (Cybersecurity Evaluation Tool)** desarrollada por CISA, seleccionando el marco **NIST CSF 2.0** como referencia principal. El procedimiento seguido fue el siguiente:

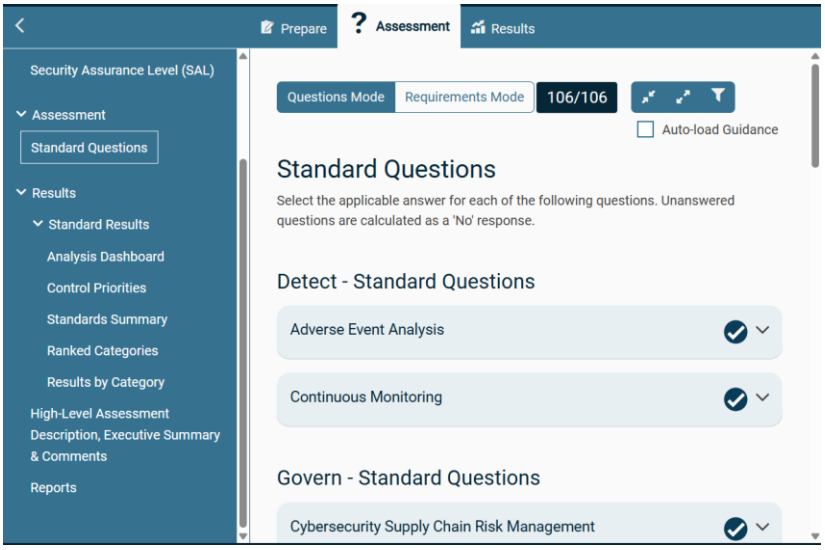
A. **Creación del Assessment:** Se inició un nuevo proyecto en CSET, configurando como estándar de evaluación el *NIST Cybersecurity Framework 2.0*.



B. Definición del Alcance: Se ingresó la información de la infraestructura evaluada, incluyendo entornos IT, OT e IoT, según la descripción del caso práctico.

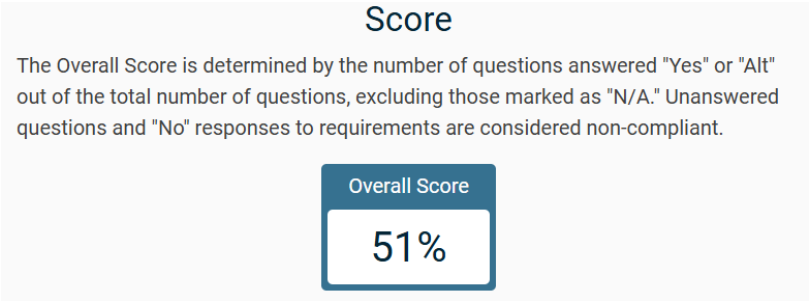


C. Evaluación de Controles: Se respondieron las preguntas y controles correspondientes a las cinco funciones del NIST CSF: *Identify, Protect, Detect, Respond* y *Recover*.

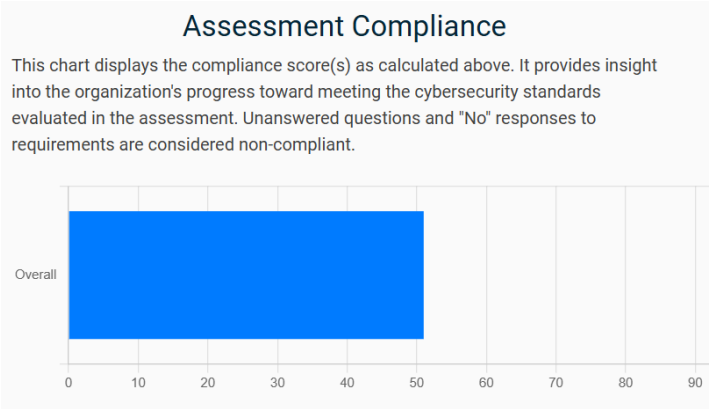


D. Generación de Resultados: CSET generó automáticamente los gráficos, matrices de cumplimiento, niveles de madurez y brechas identificadas.

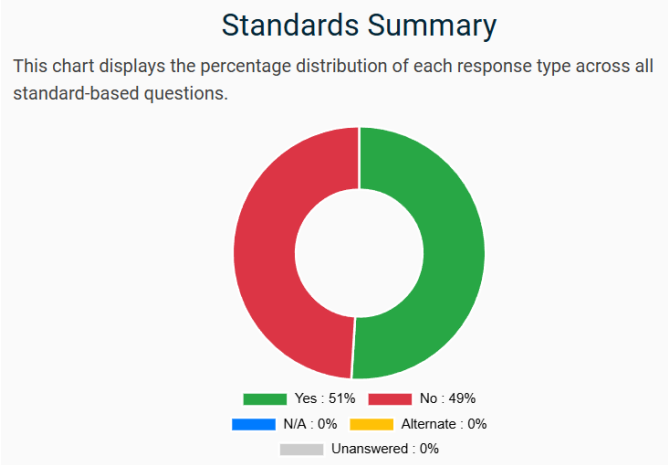
a. Puntuación



b. Cumplimiento de la evaluación

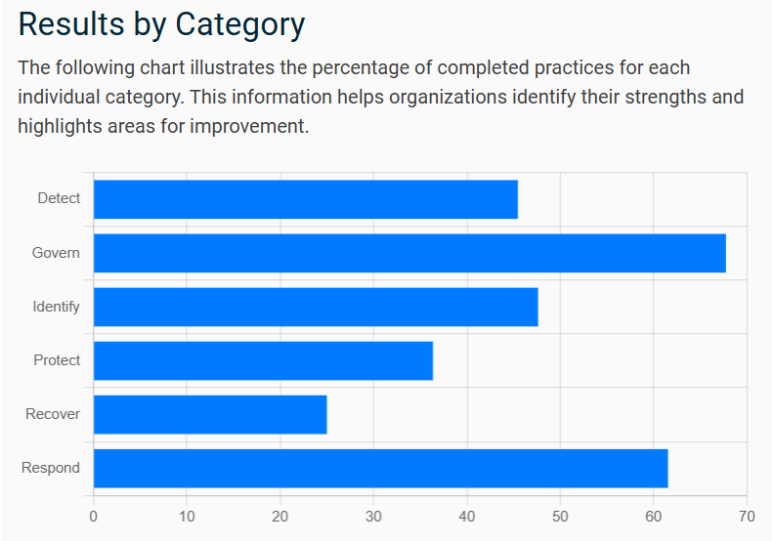


c. Resumen de estándares



Answer	Number	Total	Percent
Yes	54	106	51%
No	52	106	49%
N/A	0	0	0%
Alternate	0	0	0%
Unanswered	0	0	0%

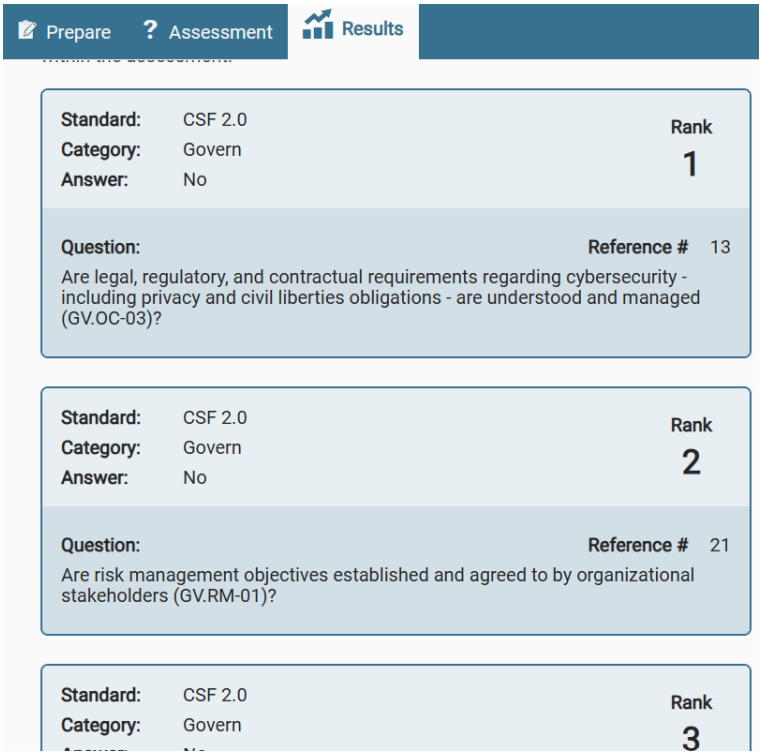
d. Resultados por categoría



CSF 2.0

Category	Passed	Total	Percent
Detect	5	11	45%
Govern	21	31	68%
Identify	10	21	48%
Protect	8	22	36%
Recover	2	8	25%
Respond	8	13	62%

e. Prioridades de control



E. Análisis Posterior: Los resultados obtenidos fueron interpretados para determinar el nivel actual de cumplimiento y priorizar las áreas de mejora.

1.6 Resultados del Assessment

El assessment realizado mediante la herramienta CSET evaluó los controles asociados al marco NIST Cybersecurity Framework (CSF) 2.0, registrando un total de 106 controles distribuidos entre las funciones principales del framework. Los resultados muestran un balance

entre controles implementados (**Y = Yes**) y no implementados (**N = No**), lo cual permite identificar el nivel de madurez de la organización en cada área evaluada.

En términos globales, el resumen de respuestas fue el siguiente:

- **Controles implementados (Y): 54**
- **Controles no implementados (N): 52**

Este resultado evidencia que la organización posee avances importantes en algunas áreas, pero aún mantiene brechas significativas que deben ser atendidas para cumplir con los requisitos de la alianza propuesta.

1.6.1 Conclusión del análisis de resultados

El assessment evidencia que la organización posee un nivel de madurez mixto: mientras que la función Govern muestra avances notables, las funciones **Protect**, **Detect** y especialmente **Recover** presentan brechas críticas que requieren atención prioritaria.

En general, la distribución casi equitativa entre controles implementados y no implementados (54 vs. 52) indica un *nivel de madurez intermedio*, pero insuficiente para cumplir estándares internacionales sin un plan de mejora inmediato.

Estos resultados servirán como base para el análisis de cumplimiento, la identificación de brechas y la construcción del plan de acción en los apartados siguientes.

1.7 Cumplimiento General

El análisis global del assessment basado en el marco NIST CSF 2.0 muestra que la organización posee un *nivel de cumplimiento intermedio*, reflejado en una distribución casi equilibrada entre controles implementados e incumplidos. De los 106 controles evaluados, 54 se encuentran implementados (Y) y 52 no implementados (N), lo que indica que la organización ha iniciado esfuerzos de alineación con el framework, pero aún mantiene brechas importantes que deben ser abordadas de forma prioritaria.

El área con mejor desempeño corresponde a la función **Govern (GV)**, que presenta la mayor cantidad de controles implementados, evidenciando que existe un marco inicial de políticas, lineamientos y estructuras de gestión. No obstante, las funciones **Protect (PR)** y **Recover (RC)**

obtuvieron los niveles de cumplimiento más bajos, lo que resalta debilidades significativas en los controles de protección, continuidad del negocio y recuperación ante incidentes.

En términos generales, el cumplimiento actual revela que la organización se encuentra en un *nivel de madurez parcial*, con mecanismos básicos establecidos pero sin consolidación completa en áreas críticas como monitoreo, protección de activos clave, gestión de incidentes y resiliencia operativa. Este resultado confirma la necesidad de fortalecer procesos, formalizar controles faltantes y priorizar la implementación de capacidades clave antes de la auditoría externa requerida por el potencial socio comercial.

1.8 Cumplimiento por Categorías

El assessment permitió identificar el nivel de cumplimiento en cada una de las funciones y categorías del NIST CSF 2.0, basándose en los controles marcados como implementados (**Y**) y no implementados (**N**) dentro del archivo exportado desde CSET.

A continuación, se presenta un resumen de cumplimiento por cada categoría principal del framework:

1.8.1 Govern (GV)

21 controles implementados – 10 controles no implementados

Esta categoría presenta el mayor nivel de cumplimiento, evidenciando que la organización cuenta con políticas iniciales, marcos de gestión y cierto nivel de gobernanza formal. Sin embargo, aún falta fortalecer lineamientos estratégicos y procesos de evaluación continua.

1.8.2 Identify (ID)

10 controles implementados – 11 controles no implementados

El cumplimiento es intermedio. Existen esfuerzos iniciales en inventarios, reconocimiento de activos y documentación parcial, pero persisten debilidades en la gestión de riesgos, análisis de impacto y clasificación de información.

1.8.3 Protect (PR)

8 controles implementados – 14 controles no implementados

La categoría de protección muestra un nivel bajo de cumplimiento. Faltan controles fundamentales como mecanismos robustos de control de acceso, protección de datos, seguridad en endpoints, autenticación avanzada y procesos de gestión de identidades.

1.8.4 Detect (DE)

5 controles implementados – 6 controles no implementados

La capacidad de detección es limitada. Aunque existe algún nivel de monitoreo o registro básico, la organización carece de herramientas formales como SIEM, monitoreo continuo, correlación de eventos y alertamiento temprano.

1.8.5 Respond (RS)

8 controles implementados – 5 controles no implementados

El nivel de cumplimiento es aceptable y muestra que existen algunos elementos de respuesta a incidentes. Sin embargo, aún falta formalizar roles, mejorar la comunicación interna y reforzar los procesos posteriores al incidente.

1.8.6 Recover (RC)

2 controles implementados – 6 controles no implementados

Esta es la categoría más débil de todas. La organización no cuenta con un Plan de Continuidad del Negocio (BCP) ni un Plan de Recuperación ante Desastres (DRP) suficientemente establecido o documentado, lo que aumenta significativamente el impacto potencial de un incidente mayor.

1.9 Brechas Identificadas

A partir de los resultados obtenidos en el assessment NIST CSF 2.0, se identificaron las principales brechas que afectan la postura de ciberseguridad de la organización. Estas brechas se derivan del análisis de los 52 controles no implementados registrados en el archivo CSET exportado.

A continuación se presentan las brechas más relevantes, organizadas según las funciones del framework:

1.9.1 Brechas en Govern (GV)

Aunque esta función posee un nivel relativamente alto de cumplimiento, se identifican brechas importantes relacionadas con:

- Falta de revisión periódica de políticas y lineamientos.
- Ausencia de mecanismos formales de evaluación continua de ciberseguridad.
- Necesidad de fortalecer el control estratégico sobre proveedores y terceros.

1.9.2 Brechas en Identify (ID)

Las principales brechas en esta función incluyen:

- Inventario incompleto o no actualizado de activos IT, OT e IoT.
- Clasificación insuficiente de información crítica.
- Gestión de riesgos sin metodologías formales ni documentación consistente.
- Falta de análisis de impacto para procesos esenciales del negocio.

1.9.3 Brechas en Protect (PR) — Una de las áreas más críticas

Entre las brechas destacadas se encuentran:

- Controles de acceso insuficientes o no estandarizados.
- Ausencia de autenticación multifactor (MFA) en sistemas claves.
- Falta de políticas formales de protección de datos sensibles.
- Mecanismos débiles de seguridad en endpoints y redes internas.
- Carencia de procesos de hardening y configuración segura de sistemas.

1.9.4 Brechas en Detect (DE)

Las brechas en esta función revelan capacidades limitadas de monitoreo:

- No existe SIEM ni correlación de eventos.
- Monitoreo de logs inconsistente o inexistente.
- Ausencia de alertas tempranas ante anomalías o actividades sospechosas.
- Falta de procedimientos para la detección continua de amenazas.

1.9.5 Brechas en Respond (RS)

Aunque hay controles implementados, persisten brechas relevantes:

- Roles y responsabilidades de respuesta a incidentes no totalmente definidos.
- Procesos incompletos de comunicación interna durante incidentes.
- Falta de documentación estructurada del proceso de manejo de incidentes.

1.9.6 Brechas en Recover (RC) — La función más débil

Las brechas más críticas se encuentran aquí:

- No existe un Plan de Continuidad del Negocio (BCP) formal.
- Absencia de un Plan de Recuperación ante Desastres (DRP).
- Falta de pruebas periódicas de recuperación.
- Procesos de restauración de servicios no documentados.

1.10 Riesgos Asociados

Las brechas identificadas en el assessment NIST CSF 2.0 representan riesgos importantes para la organización, tanto en términos operativos como estratégicos. Estos riesgos se derivan directamente de los 52 controles que no se encuentran implementados según los resultados del archivo CSET exportado.

A continuación se presentan los principales riesgos asociados, agrupados según las funciones del framework:

1.10.1 Riesgos asociados a Govern (GV)

- **Desalineación estratégica:** La falta de procesos formales de revisión y mejora continua puede provocar que la estrategia de ciberseguridad no responda adecuadamente a amenazas emergentes.
- **Riesgos con terceros:** La ausencia de controles de gobernanza sobre proveedores puede facilitar brechas a través de integraciones no supervisadas.

1.10.2 Riesgos asociados a Identify (ID)

- **Exposición no identificada:** Inventarios incompletos implican desconocimiento de activos críticos, aumentando la probabilidad de que sistemas vulnerables pasen inadvertidos.
- **Clasificación deficiente de datos:** Sin clasificación formal, datos sensibles pueden ser gestionados sin las medidas de protección adecuadas.

- **Evaluación de riesgos insuficiente:** La falta de metodologías formales impide priorizar amenazas, afectando la toma de decisiones.

1.10.3 Riesgos asociados a Protect (PR)

- **Accesos no controlados:** La carencia de controles robustos de autenticación y autorización incrementa la posibilidad de accesos no autorizados.
- **Compromiso de datos sensibles:** Controles insuficientes de protección de datos pueden provocar fugas, pérdidas o manipulación de información crítica.
- **Endpoints vulnerables:** La falta de hardening y protección centralizada incrementa el riesgo de malware, ransomware y ataques dirigidos.

1.10.4 Riesgos asociados a Detect (DE)

- **Falta de visibilidad:** Sin monitoreo continuo o SIEM, incidentes pueden pasar desapercibidos durante largos periodos.
- **Incidentes sin alerta:** La ausencia de correlación de eventos limita la capacidad de identificar ataques complejos.
- **Respuesta tardía:** La demora en detectar anomalías aumenta la superficie de daño potencial.

1.10.5 Riesgos asociados a Respond (RS)

- **Caos operativo ante incidentes:** La falta de roles, procedimientos y comunicación definida puede generar respuestas desorganizadas durante ataques.
- **Mayor impacto del incidente:** Sin un proceso claro de contención, los daños pueden escalar rápidamente.
- **Dependencia de acciones manuales no documentadas:** Dificulta la consistencia y calidad de la respuesta.

1.10.6 Riesgos asociados a Recover (RC)

- **Interrupción prolongada del negocio:** La ausencia de BCP y DRP puede provocar tiempos de recuperación muy elevados.
- **Pérdida irreversible de datos:** Sin procesos documentados de restauración, existe riesgo de pérdida permanente de información crítica.

- **Impacto financiero y reputacional severo:** La incapacidad para recuperarse de un incidente puede afectar la continuidad de la organización y su relación con clientes y socios.

1.11 Prioridades Críticas

A partir del análisis de cumplimiento, brechas y riesgos identificados en el assessment NIST CSF 2.0, se establecieron las **cinco prioridades críticas** que requieren atención inmediata para fortalecer la postura de ciberseguridad de la organización. Estas prioridades se basan en los controles no implementados identificados en el archivo exportado desde CSET.

Las prioridades seleccionadas corresponden a las áreas con mayor impacto potencial sobre la continuidad operativa, la detección de amenazas y la resiliencia institucional.

1.11.1 Prioridad 1 — Implementación del Plan de Recuperación ante Desastres (DRP) y Plan de Continuidad del Negocio (BCP)

La función **Recover (RC)** es la más débil del assessment. La ausencia de planes formales afecta la capacidad de la organización para restaurar servicios críticos tras un incidente.

Impacto: Alto — Riesgo de interrupción total de operaciones.

Urgencia: Inmediata.

1.11.2 Prioridad 2 — Fortalecimiento de controles de protección (Protect – PR)

Múltiples controles PR no están implementados, incluyendo autenticación multifactor (MFA), hardening, protección de datos y control de acceso.

Impacto: Alto — Incrementa la probabilidad de accesos no autorizados y fugas de información.

Urgencia: Alta.

1.11.3 Prioridad 3 — Establecimiento de capacidades de monitoreo y detección (Detect – DE)

La falta de SIEM, correlación de eventos y monitoreo continuo limita la visibilidad frente a amenazas internas y externas.

Impacto: Alto — Incrementa riesgo de detección tardía de incidentes.

Urgencia: Alta.

1.11.4 Prioridad 4 — Formalización del proceso de gestión de incidentes (Respond – RS)

Si bien existen algunos controles implementados, faltan roles claramente definidos, mecanismos de comunicación y procedimientos documentados.

Impacto: Medio-Alto — Una respuesta deficiente aumenta el alcance del daño.

Urgencia: Alta.

1.11.5 Prioridad 5 — Consolidación del inventario y clasificación de activos (Identify – ID)

Inventarios incompletos y ausencia de clasificación generan falta de visibilidad sobre sistemas críticos.

Impacto: Medio — No se puede proteger lo que no se conoce.

Urgencia: Media-Alta.

1.12 Plan de Acción

Con base en las brechas, riesgos y prioridades críticas identificadas durante el assessment NIST CSF 2.0, se definió el siguiente Plan de Acción enfocado en fortalecer las capacidades de protección, detección, respuesta y recuperación de la organización. Este plan integra las cinco prioridades críticas identificadas y establece las acciones necesarias, responsables, plazos y beneficios esperados para avanzar hacia un nivel de madurez adecuado.

Prioridad	Acción Requerida	Responsable	Plazo Estimado	Beneficio Esperado
1	Desarrollar e implementar un **DRP (Disaster Recovery Plan)** y un **BCP (Business Continuity Plan)** completos.	Dirección de TI / Gerencia General	2–3 meses	Garantiza recuperación operativa, reduce interrupciones y protege la continuidad del negocio.
2	Fortalecer los controles de **Protección (PR)**: MFA, políticas de acceso, hardening, cifrado, seguridad en endpoints.	Seguridad Informática / TI	1–2 meses	Reduce la probabilidad de accesos no autorizados y fugas de información.

3	Implementar capacidades de **monitoreo y detección**, incluyendo SIEM, alertas automáticas y correlación de eventos.	SOC / TI	2–4 meses	Mejora la visibilidad de amenazas y reduce el tiempo de detección de incidentes.
4	Formalizar el **Proceso de Gestión de Incidentes**, definiendo roles, procedimientos, comunicación interna y bitácoras.	Seguridad Informática	1 mes	Permite una respuesta organizada y reduce el impacto ante incidentes.
5	Crear y mantener un **Inventario y Clasificación de Activos** para entornos IT, OT e IoT.	TI / OT	1 mes	Identifica activos críticos y permite aplicar controles adecuados en cada uno.

Capítulo 2

Auditoría Firewall Fortigate 2000E

2.1 Objetivos de la Auditoría

El objetivo de esta auditoría es evaluar la configuración y el nivel de seguridad del firewall Fortigate 2000E implementado en el banco XYZBA. Se busca identificar brechas de seguridad, validar el cumplimiento de estándares internacionales (ISO 27001 y NIST SP 800-41), y proponer mejoras para fortalecer la protección de la infraestructura crítica. Además, se promueve la adopción de buenas prácticas como la firma de acuerdos de confidencialidad antes de iniciar la auditoría.

2.2 Alcance de la Auditoría

La auditoría se limita a:

- Revisar la configuración actual del firewall Fortigate 2000E en el ambiente demo.
- Analizar políticas de acceso, reglas de filtrado, segmentación de red, y mecanismos de protección contra amenazas.
- Evaluar el cumplimiento de controles definidos por los marcos ISO 27001 y NIST SP 800-41.
- Identificar riesgos y proponer acciones de remediación.
- No se realizarán cambios en el ambiente productivo ni pruebas invasivas.

2.3 Marco de Trabajo Aplicado (ISO 27001 / NIST SP 800-41)}

La auditoría se basa en:

- **ISO 27001:** Revisión de controles de seguridad de la información, gestión de accesos, protección de activos, y respuesta ante incidentes.
- **NIST SP 800-41:** Evaluación de la gestión de firewalls, configuración segura, monitoreo, y mantenimiento.

En esta sección puedes incluir una tabla comparativa de los controles relevantes de ambos marcos y cómo se aplican al firewall.

2.4 Plan de Trabajo (Trello/Planner)

2.4.1 Descripción:

Para la gestión y seguimiento de las actividades de la auditoría del firewall Fortigate 2000E, se utilizó la herramienta Trello (o Planner, según tu elección). El tablero se estructuró en listas que representan el estado de las tareas: “Por hacer”, “En progreso” y “Finalizado”. Cada tarea fue asignada con fechas de inicio y fin, responsables y, cuando corresponde, adjuntos como capturas de pantalla o documentos de soporte.

2.4.2 Estructura del tablero:

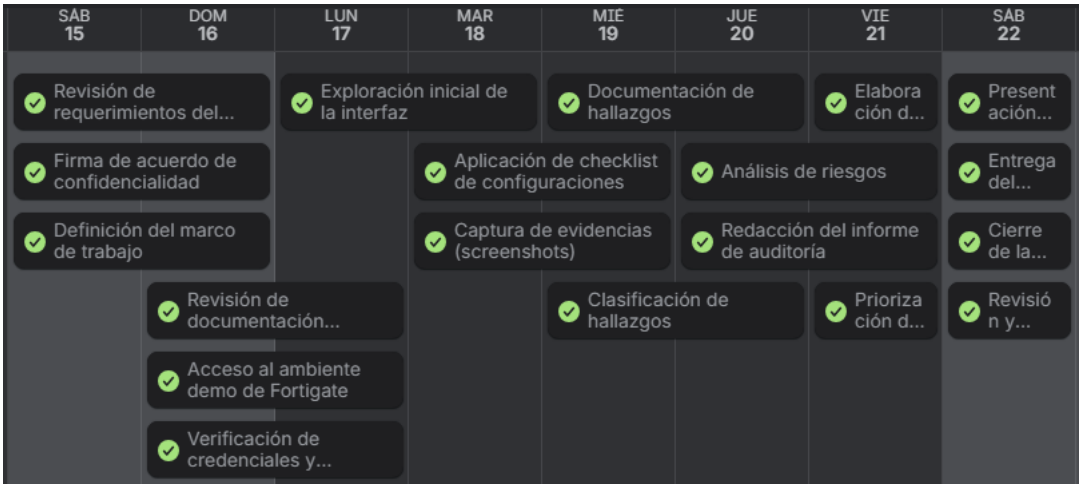
- **Listas:**
  - Por hacer
  - En progreso
  - Finalizado
- **Tarjetas/Tareas:**
  - Revisión de requerimientos del cliente
  - Firma de acuerdo de confidencialidad
  - Definición del marco de trabajo
  - Revisión de documentación técnica
  - Acceso al ambiente demo
  - Verificación de credenciales
  - Exploración inicial
  - Aplicación de checklist
  - Captura de evidencias
  - Documentación de hallazgos
  - Clasificación de hallazgos
  - Análisis de riesgos
  - Redacción del informe
  - Elaboración del plan de remediación
  - Priorización de acciones
  - Revisión y validación
  - Presentación de resultados
  - Entrega del informe
  - Cierre de la auditoría

2.4.3 *Fechas asignadas:*

Las tareas se distribuyeron entre el 15/11 y el 22/11, asegurando el cumplimiento del cronograma y permitiendo revisiones antes de la entrega final.

2.4.4 *Tablero Trello*

Tarjeta	Lista	Etiquetas	Miembros	Fecha de vencimiento
Revisión de requerimientos del cliente	Hoy	·	·	16 nov
Firma de acuerdo de confidencialidad	Hoy	·	·	16 nov
Definición del marco de trabajo	Hoy	·	·	16 nov
Revisión de documentación técnica	Hoy	·	·	17 nov
Acceso al ambiente demo de Fortigate	Hoy	·	·	17 nov
Verificación de credenciales y permisos	Hoy	·	·	17 nov
Exploración inicial de la interfaz	Hoy	·	·	18 nov
Aplicación de checklist de configuraciones	Hoy	·	·	19 nov
Captura de evidencias (screenshots)	Hoy	·	·	19 nov
Documentación de hallazgos	Hoy	·	·	20 nov
Clasificación de hallazgos	Hoy	·	·	20 nov
Análisis de riesgos	Hoy	·	·	21 nov
Redacción del informe de auditoría	Hoy	·	·	21 nov
Elaboración del plan de remediación	Hoy	·	·	21 nov
Priorización de acciones correctivas	Hoy	·	·	21 nov
Presentación de resultados al cliente	Hoy	·	·	22 nov
Añadir ega del informe y plan de remediación	Hoy	·	·	22 nov



2.4.5 *Ventajas de la herramienta:*

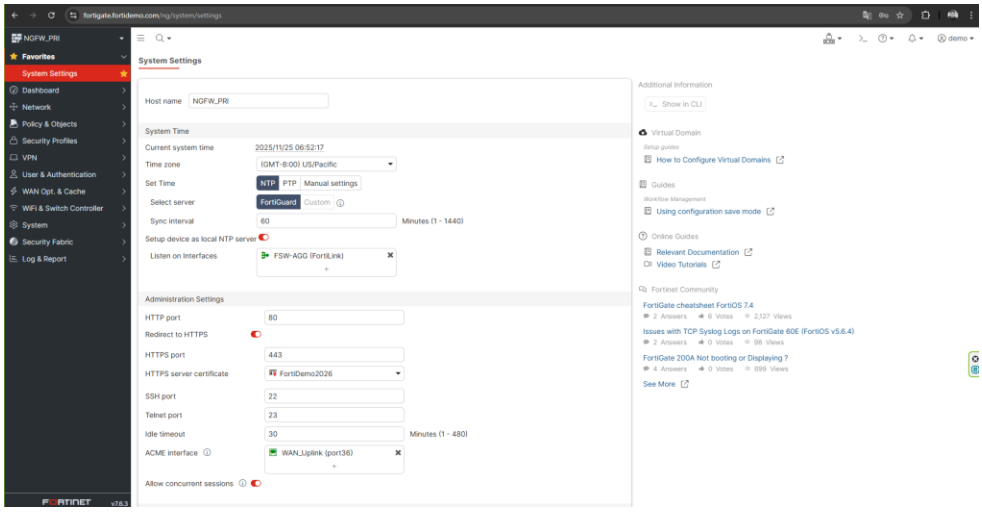
- Permite visualizar el avance de la auditoría.
- Facilita la colaboración y asignación de tareas.
- Ayuda a cumplir los plazos establecidos.
- Permite adjuntar evidencias y comentarios en cada tarea.

2.5 Desarrollo de la Auditoría

La auditoría se llevó a cabo en el ambiente demo del firewall Fortigate 2000E, siguiendo el plan de trabajo previamente definido y utilizando como referencia los controles de los marcos ISO 27001 y NIST SP 800-41. El proceso incluyó la revisión técnica de configuraciones, la aplicación de un checklist, la captura de evidencias y el registro de hallazgos.

2.5.1 Acceso al ambiente demo

- Se accedió al entorno de demostración proporcionado por Fortigate (https://fortigate.fortidemo.com/).
- Se verificó el acceso y las credenciales necesarias para explorar todas las funcionalidades relevantes del firewall.



2.5.2 Revisión de configuraciones clave

- Se exploraron las principales secciones del firewall:
  - Políticas de firewall y reglas de acceso.
  - Configuración de autenticación y autorización.
  - Segmentación de red y configuración de VPN.
  - Módulos de protección contra amenazas (IPS, antivirus).
  - Registro y monitoreo de eventos.

2.5.3 Aplicación del checklist técnico

Se aplicó un checklist técnico basado en los controles de ISO 27001 y NIST SP 800-41. Cada ítem fue verificado directamente en el ambiente demo del firewall Fortigate 2000E. Para

cada configuración revisada, se documentó el cumplimiento o la desviación, y se capturaron evidencias visuales (screenshots) para respaldar los hallazgos. El checklist incluyó aspectos como reglas de acceso, autenticación, segmentación de red, actualizaciones, monitoreo y protección contra amenazas.

2.5.4 Captura y registro de evidencias

Durante la auditoría, se realizó la captura sistemática de evidencias visuales en el ambiente demo de Fortigate 2000E. Estas evidencias incluyen configuraciones relevantes, hallazgos detectados y cualquier desviación respecto a las buenas prácticas. Las capturas fueron organizadas y registradas para respaldar el análisis y las conclusiones del informe.

2.5.5 Documentación de hallazgos

Los hallazgos identificados durante la auditoría fueron documentados de manera estructurada, clasificando cada uno según su nivel de criticidad y relacionándolos con los controles del marco de trabajo. Cada hallazgo cuenta con su respectiva evidencia visual, la cual será presentada en la sección de hallazgos detallados.

2.5.6 Análisis preliminar de riesgos

Se realizó un análisis preliminar de los riesgos asociados a los hallazgos detectados, evaluando el impacto y la probabilidad de cada uno. Este análisis servirá como base para la priorización de acciones de remediación, y será ampliado en la sección de análisis de riesgos detallados.

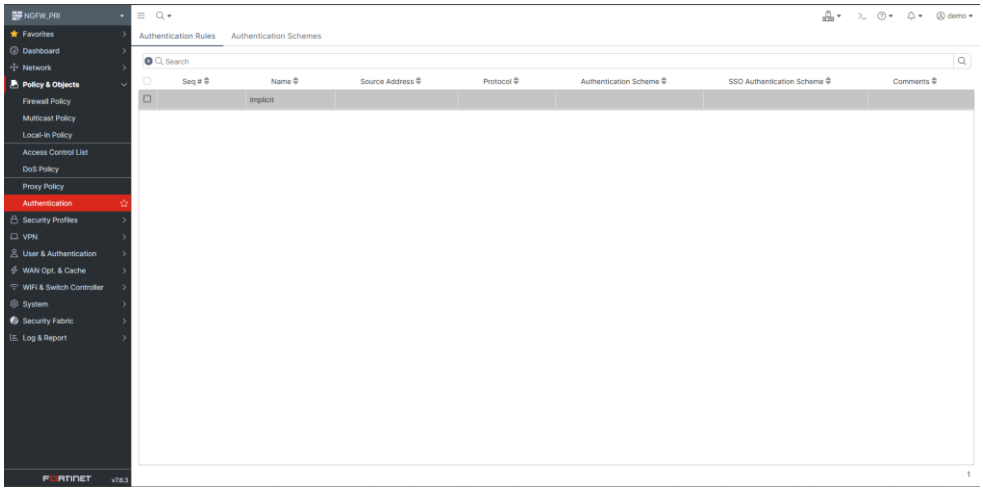
2.6 Checklist de Configuraciones

2.6.1 Reglas de acceso y filtrado (Firewall Policies)

La configuración muestra múltiples reglas de acceso entre diferentes segmentos de red (DMZ, Staff, Teachers, Students, SAP HANA, WAN uplink). Se observa que algunas reglas permiten tráfico “any”, lo que puede representar un riesgo si no está justificado. Es recomendable revisar y restringir estas reglas según la necesidad real, aplicando perfiles de seguridad y habilitando el registro de eventos.

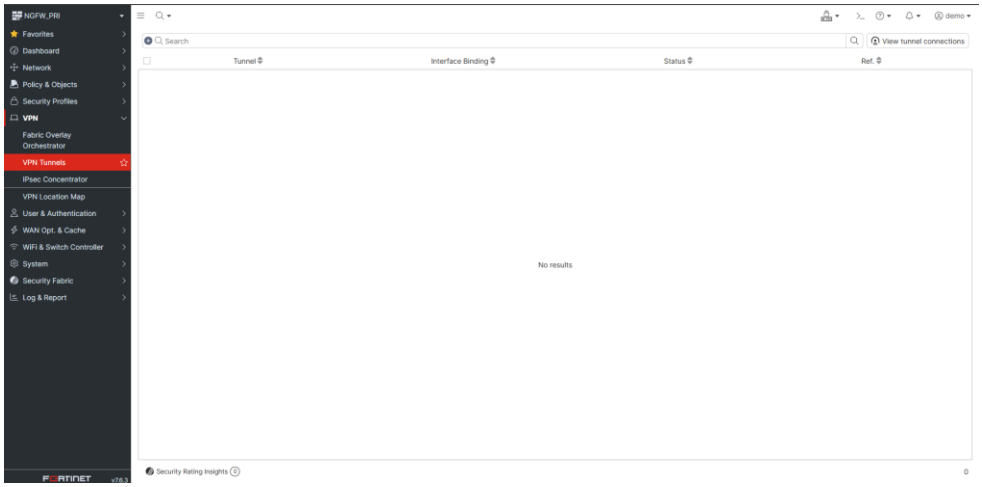
2.6.2 Políticas de autenticación y autorización

La evidencia muestra la sección de “Authentication Rules”, donde actualmente no hay reglas configuradas. Esto indica que no se han definido esquemas de autenticación específicos, lo que puede limitar el control de acceso granular. Se recomienda implementar reglas de autenticación para fortalecer la seguridad.



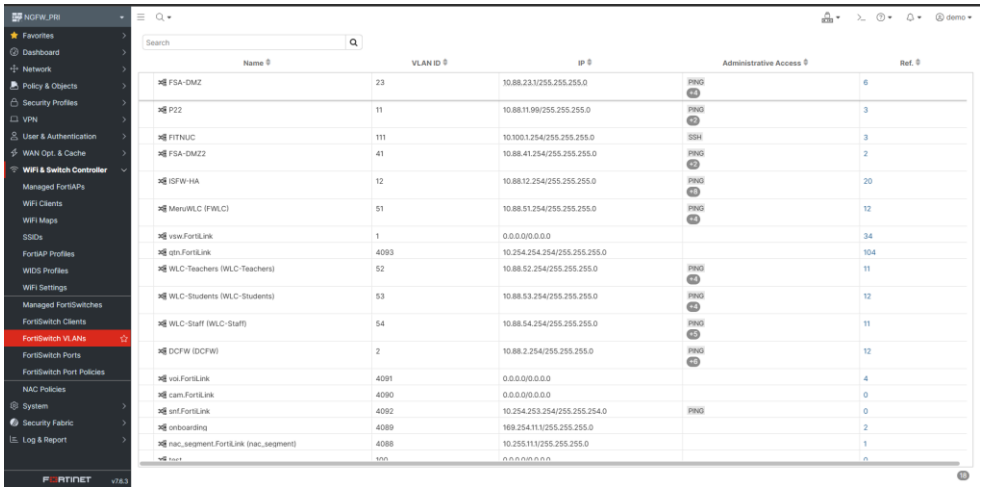
2.6.3 Configuración de VPN (IPSec/SSL)

La sección “VPN Events” indica que no existen túneles configurados actualmente. Esto puede significar que no hay conexiones VPN activas, lo cual es relevante si se requiere acceso remoto seguro. Se recomienda revisar la necesidad de VPN y configurar túneles según las políticas de la organización.



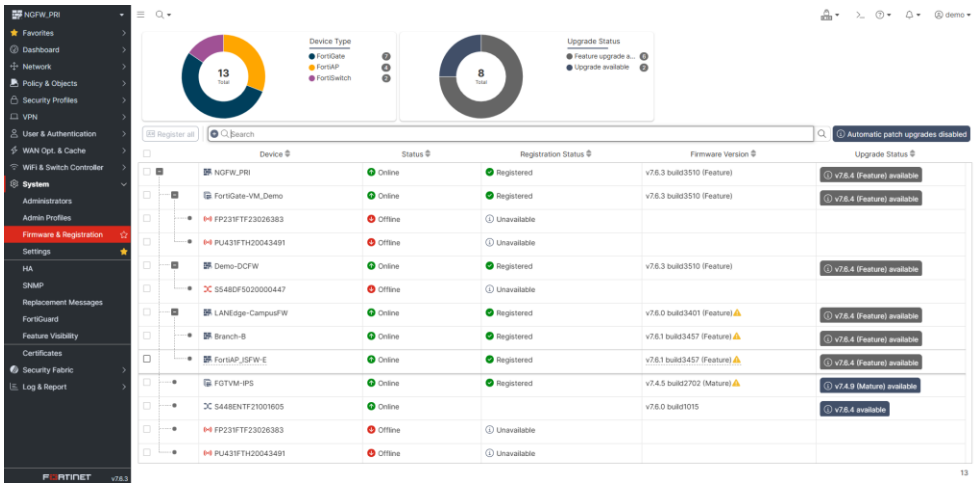
2.6.4 Segmentación de red (VLANs, zonas)

La evidencia muestra la configuración de múltiples VLANs y zonas, cada una con su respectiva dirección IP y acceso administrativo. Esto indica una segmentación adecuada de la red, permitiendo separar los diferentes grupos y servicios. Se recomienda revisar los permisos de administración y asegurar que cada segmento tenga controles apropiados.



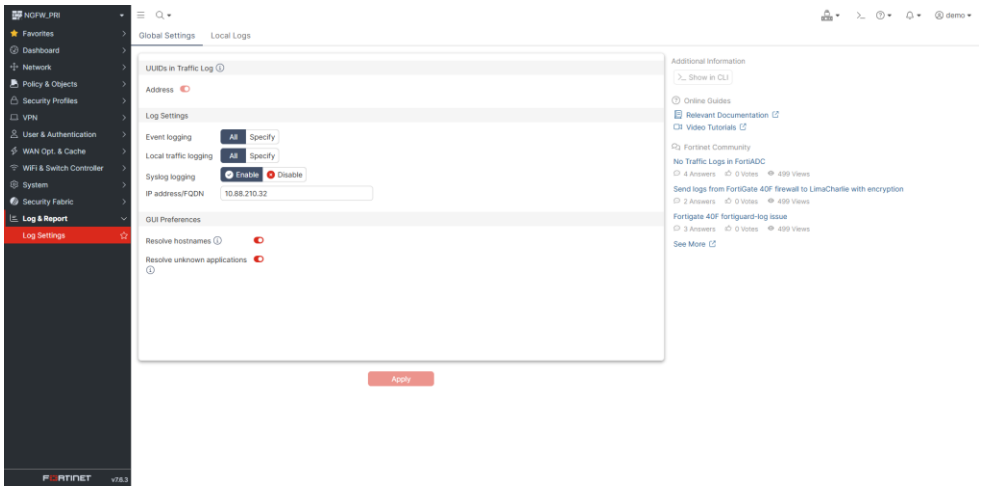
2.6.5 Actualización y parches del sistema (Firmware)

La sección de “Firmware & Registration” muestra el estado de actualización de los dispositivos. La mayoría están actualizados, aunque algunos presentan advertencias de parches pendientes. Es fundamental mantener el firmware actualizado para proteger contra vulnerabilidades conocidas.



2.6.6 *Monitoreo y registro de eventos (Logs)*

La evidencia muestra la configuración de logs, donde el registro de eventos está habilitado y se especifica el servidor de syslog. Esto es positivo para la auditoría y el monitoreo continuo. Se recomienda revisar que todos los eventos críticos estén siendo registrados.



2.6.7 *Protección contra amenazas (IPS, Antivirus, Web Filtering)*

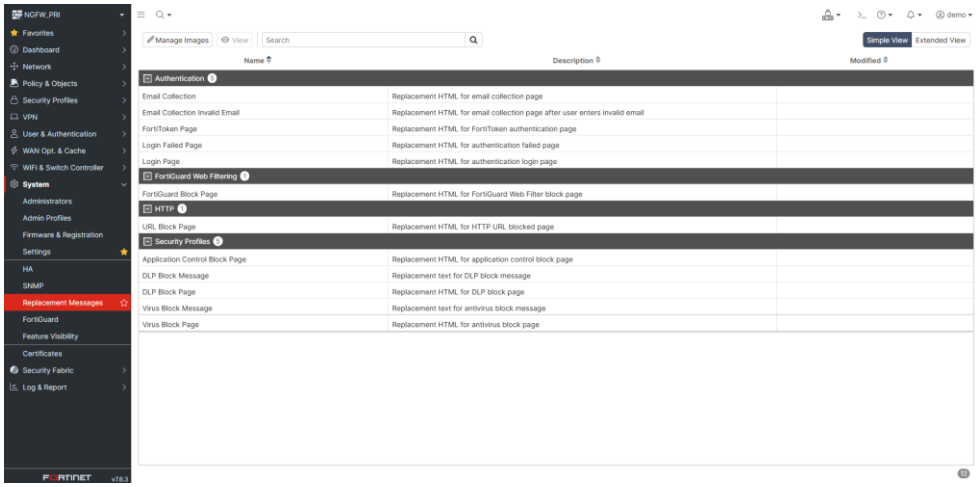
La sección de “Security Profiles” muestra la configuración de perfiles de protección, incluyendo web filtering y antivirus. Se observa que existen perfiles por defecto y personalizados. Es recomendable revisar que todos los perfiles estén correctamente aplicados a las reglas relevantes.

2.6.8 Gestión de usuarios y roles

La evidencia muestra la configuración de servidores LDAP para la autenticación de usuarios. Esto permite una gestión centralizada de usuarios y roles, lo cual es una buena práctica. Se recomienda revisar los permisos asignados y la integración con otros sistemas de autenticación.

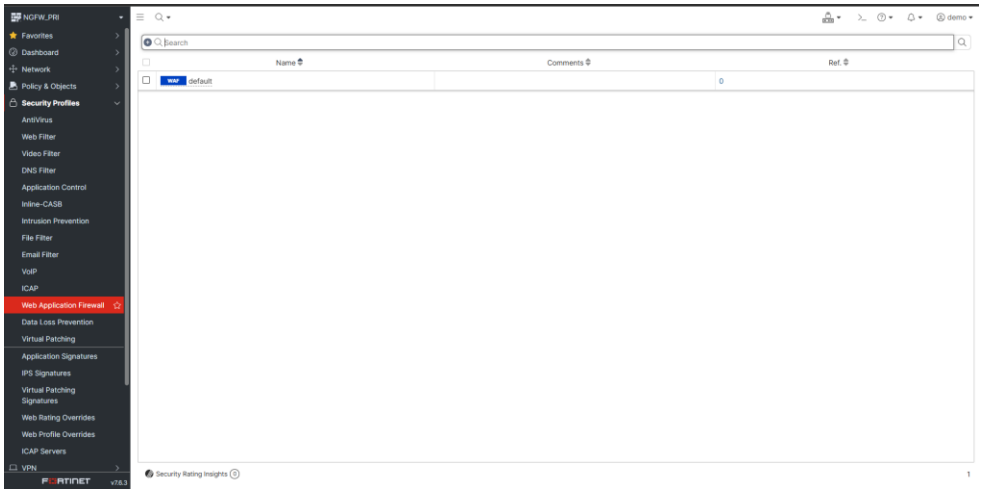
2.6.9 Configuración de alertas y notificaciones

La sección de “Replacement Messages” muestra la personalización de mensajes de alerta y notificación para diferentes eventos de seguridad. Esto ayuda a informar a los usuarios sobre bloqueos o incidentes. Se recomienda mantener estos mensajes actualizados y claros.



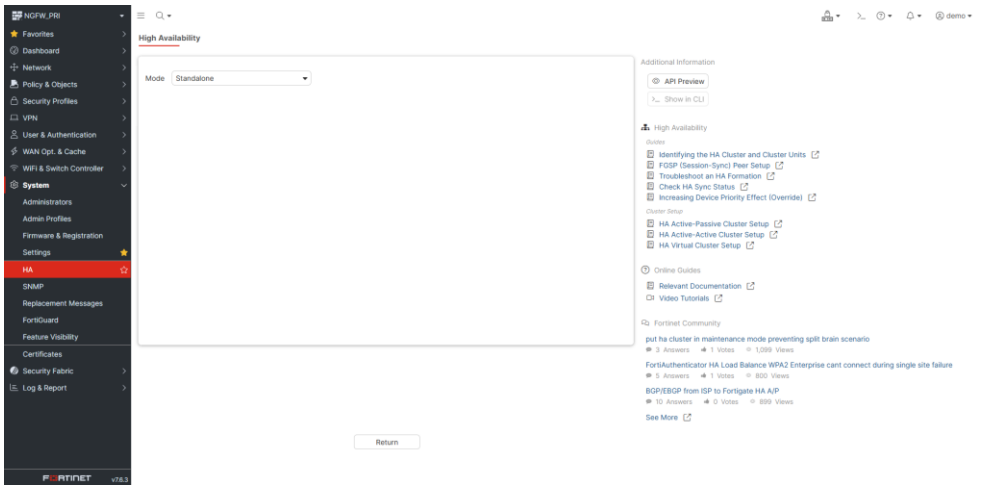
2.6.10 Políticas de acceso a la administración web

La evidencia muestra la configuración de políticas para el acceso a la administración web, donde existe una política por defecto. Es recomendable revisar y restringir el acceso administrativo solo a usuarios autorizados y desde ubicaciones seguras.



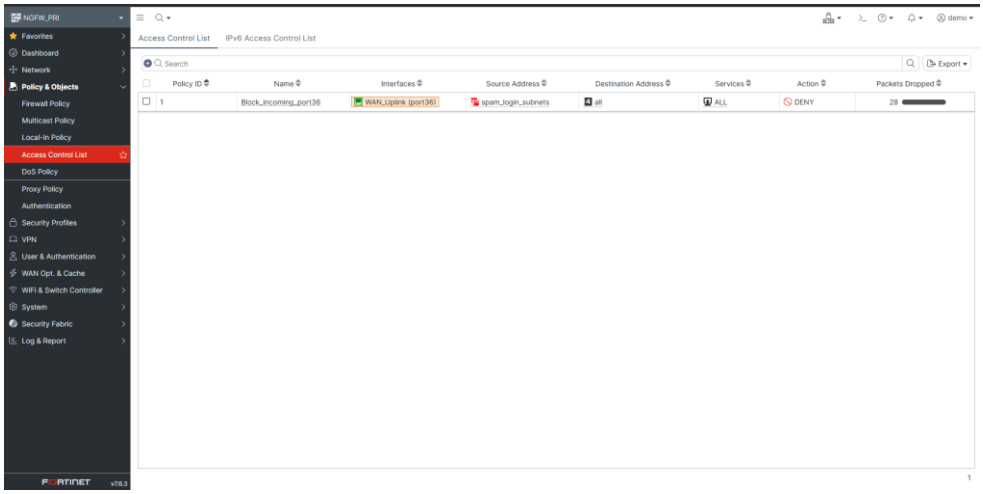
2.6.11 Configuración de alta disponibilidad (HA)

La sección de “High Availability” muestra que el modo actual es “Standalone”, es decir, no hay configuración de HA activa. Si la continuidad del servicio es crítica, se recomienda implementar alta disponibilidad.



2.6.12 Políticas de acceso a servicios críticos (DNS, DHCP, etc.)

La evidencia muestra una lista de control de acceso (ACL) para servicios críticos, donde se observa una política que bloquea el acceso desde una fuente específica a la WAN uplink. Es recomendable revisar y ajustar estas políticas para proteger los servicios esenciales.



2.7 Hallazgos en el Ambiente Demo

A continuación, se presentan los principales hallazgos identificados durante la auditoría en el ambiente demo de Fortigate 2000E. Cada hallazgo incluye una breve descripción, el impacto potencial y la evidencia visual correspondiente.

A. Reglas de acceso y filtrado (Firewall Policies)

a. **Hallazgo:** Se detectaron reglas que permiten tráfico “any” entre diferentes segmentos de red, lo que puede representar un riesgo de acceso no autorizado si no está justificado.

b. **Impacto:** Alto riesgo de exposición y acceso indebido.

B. Políticas de autenticación y autorización

a. **Hallazgo:** No existen reglas de autenticación configuradas, lo que limita el control granular sobre el acceso a recursos críticos.
b. **Impacto:** Riesgo medio de acceso no controlado.

C. Configuración de VPN (IPSec/SSL)

a. **Hallazgo:** No se encontraron túneles VPN configurados, lo que puede limitar el acceso remoto seguro para usuarios autorizados.
b. **Impacto:** Riesgo bajo si no se requiere acceso remoto, pero alto si es necesario y no está implementado.

D. Segmentación de red (VLANs, zonas)

a. **Hallazgo:** La segmentación de red está implementada con múltiples VLANs y zonas, lo que es positivo. Sin embargo, se recomienda revisar los permisos administrativos para cada segmento.
b. **Impacto:** Riesgo bajo si los permisos están correctamente gestionados.

E. Actualización y parches del sistema (Firmware)

a. **Hallazgo:** Algunos dispositivos presentan advertencias de parches pendientes, lo que puede exponer el sistema a vulnerabilidades conocidas.
b. **Impacto:** Riesgo alto de explotación de vulnerabilidades.

F. Monitoreo y registro de eventos (Logs)

a. **Hallazgo:** El registro de eventos está habilitado y se especifica el servidor de syslog, lo que es positivo para la auditoría y el monitoreo.
b. **Impacto:** Riesgo bajo, pero se recomienda revisar que todos los eventos críticos estén siendo registrados.

G. Protección contra amenazas (IPS, Antivirus, Web Filtering)

a. **Hallazgo:** Se encuentran configurados perfiles de protección, incluyendo web filtering y antivirus. Es necesario revisar que estos perfiles estén aplicados a todas las reglas relevantes.
b. **Impacto:** Riesgo medio si no se aplican correctamente a todas las reglas.

H. Gestión de usuarios y roles

a. **Hallazgo:** Se utiliza LDAP para la autenticación de usuarios, lo que permite una gestión centralizada. Es importante revisar los permisos asignados.
b. **Impacto:** Riesgo bajo si la gestión de permisos es adecuada.

I. Configuración de alertas y notificaciones

a. **Hallazgo:** Se han personalizado los mensajes de alerta y notificación, lo que mejora la comunicación ante incidentes de seguridad.
b. **Impacto:** Riesgo bajo.

J. Políticas de acceso a la administración web

a. **Hallazgo:** Existe una política por defecto para el acceso a la administración web. Se recomienda restringir el acceso administrativo solo a usuarios autorizados y desde ubicaciones seguras.
b. **Impacto:** Riesgo medio si el acceso no está suficientemente restringido.

K. Configuración de alta disponibilidad (HA)

a. **Hallazgo:** El modo actual es “Standalone”, sin configuración de alta disponibilidad. Si la continuidad del servicio es crítica, se recomienda implementar HA.

b. **Impacto:** Riesgo medio de interrupción del servicio ante fallos.

L. Políticas de acceso a servicios críticos (DNS, DHCP, etc.)

a. **Hallazgo:** Se observa una política que bloquea el acceso desde una fuente específica a la WAN uplink, lo que ayuda a proteger servicios esenciales.

b. **Impacto:** Riesgo bajo si las políticas están correctamente configuradas.

2.8 Análisis de Riesgo de Configuración

A continuación, se presenta el análisis de riesgo asociado a cada hallazgo identificado en el ambiente demo del firewall Fortigate 2000E. Para cada caso se evalúa el impacto, la probabilidad y el nivel de riesgo, lo que permite priorizar las acciones de remediación.

Hallazgo	Impacto	Probabilidad	Nivel de riesgo	Observaciones/Recomendaciones
Reglas de acceso “any”	Crítico	Alta	Muy alto	Restringir reglas y aplicar perfiles de seguridad
Sin reglas de autenticación	Alto	Media	Alto	Implementar reglas de autenticación y MFA
Sin túneles VPN configurados	Medio	Baja	Bajo/Medio	Configurar VPN si se requiere acceso remoto seguro
Segmentación de red implementada	Bajo	Baja	Bajo	Revisar permisos administrativos en cada segmento
Parches pendientes en firmware	Crítico	Alta	Muy alto	Actualizar firmware en todos los dispositivos
Logs habilitados, pero revisar eventos críticos	Medio	Media	Medio	Verificar que todos los eventos relevantes se registren
Perfiles de protección aplicados parcialmente	Alto	Media	Alto	Revisar y aplicar perfiles a todas las reglas relevantes
LDAP para gestión de usuarios	Bajo	Baja	Bajo	Revisar permisos y roles asignados
Mensajes de alerta personalizados	Bajo	Baja	Bajo	Mantener mensajes claros y actualizados
Política por defecto en administración web	Medio	Media	Medio	Restringir acceso administrativo solo a usuarios autorizados
Sin alta disponibilidad (HA)	Alto	Baja	Medio	Implementar HA si la continuidad es crítica
Políticas de acceso a servicios críticos	Bajo	Baja	Bajo	Revisar y ajustar políticas según necesidad

2.9 Plan de Remediación

A continuación, se presenta el plan de remediación para los hallazgos identificados en la auditoría del firewall Fortigate 2000E. Las acciones propuestas están priorizadas según el nivel de riesgo y buscan fortalecer la postura de seguridad de la organización.

Hallazgo	Acción recomendada	Prioridad	Responsable	Plazo estimado
Reglas de acceso “any”	Restringir reglas, aplicar el principio de mínimo privilegio y asociar perfiles de seguridad	Alta	Equipo de red	1 día
Sin reglas de autenticación	Implementar reglas de autenticación y habilitar MFA	Alta	Equipo de seguridad	2 días
Sin túneles VPN configurados	Configurar VPN para acceso remoto seguro, si es necesario	Media	Equipo de red	2 días
Segmentación de red implementada	Revisar y ajustar permisos administrativos en cada segmento	Media	Equipo de red	2 días
Parches pendientes en firmware	Actualizar firmware en todos los dispositivos	Alta	Equipo de TI	1 día
Logs habilitados, pero revisar eventos críticos	Verificar que todos los eventos relevantes se registren	Media	Equipo de seguridad	2 días
Perfiles de protección aplicados parcialmente	Revisar y aplicar perfiles de protección a todas las reglas relevantes	Alta	Equipo de seguridad	2 días
LDAP para gestión de usuarios	Revisar y ajustar permisos y roles asignados	Media	Equipo de TI	2 días
Mensajes de alerta personalizados	Mantener mensajes claros y actualizados	Baja	Equipo de seguridad	3 días
Política por defecto en administración web	Restringir acceso administrativo solo a usuarios autorizados y desde ubicaciones seguras	Alta	Equipo de TI	1 día
Sin alta disponibilidad (HA)	Implementar HA si la continuidad del servicio es crítica	Media	Equipo de TI	5 días
Políticas de acceso a servicios críticos	Revisar y ajustar políticas de acceso según necesidad	Media	Equipo de red	2 días

Capítulo 3

Acuerdo de Confidencialidad (NDA)

ACUERDO DE CONFIDENCIALIDAD Y BUEN USO DE LA INFORMACIÓN

Entre:
Banco XYZBA (en adelante, “La Entidad”)
y
Brandon Eduardo Godinez Suret (en adelante, “El Auditor”)

Objeto:
El presente acuerdo tiene como finalidad proteger la confidencialidad de la información a la que El Auditor tendrá acceso durante la auditoría externa del firewall Fortigate 2000E, así como asegurar el buen uso de los datos y documentos proporcionados por La Entidad.

Cláusulas:

A. **Confidencialidad:** El Auditor se compromete a no divulgar, compartir, copiar ni transferir a terceros ninguna información técnica, operativa, administrativa o de seguridad obtenida durante el proceso de auditoría, salvo autorización expresa y por escrito de La Entidad.
B. **Uso de la información:** Toda la información, documentos, configuraciones, capturas de pantalla y registros obtenidos durante la auditoría serán utilizados exclusivamente para los fines del proyecto y no podrán ser empleados para ningún otro propósito.
C. **Protección de datos:** El Auditor se compromete a proteger la información contra accesos no autorizados, pérdida, alteración o destrucción, aplicando las mejores prácticas de seguridad de la información.
D. **Devolución y eliminación:** Al finalizar la auditoría, El Auditor deberá devolver o eliminar toda la información proporcionada por La Entidad, incluyendo archivos digitales, documentos impresos y registros electrónicos.
E. **Vigencia:** El presente acuerdo tendrá vigencia desde la fecha de inicio de la auditoría hasta la finalización del proyecto y la entrega del informe final.
F. **Responsabilidad:** El incumplimiento de cualquiera de las cláusulas aquí establecidas podrá dar lugar a acciones legales y/o sanciones administrativas por parte de La Entidad.

Firmas:

Brandon Eduardo Godinez Suret
Auditor Externo

Representante Banco XYZBA
La Entidad

Fecha: Guatemala, 15 de noviembre de 2025

Conclusiones

La auditoría realizada sobre el firewall Fortigate 2000E y el GAP análisis de cumplimiento frente al NIST CSF 2.0 permitieron identificar el estado actual de la postura de ciberseguridad de la organización, así como las principales brechas y riesgos que deben ser atendidos para cumplir con los requisitos internacionales y fortalecer la protección de los activos críticos.

Se evidenció que la organización cuenta con avances importantes en áreas de gobernanza y gestión de políticas, pero mantiene debilidades relevantes en funciones de protección, detección, respuesta y recuperación. Las brechas más críticas se relacionan con la ausencia de un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), controles insuficientes de autenticación y protección de datos, capacidades limitadas de monitoreo y detección, y procesos de gestión de incidentes poco formalizados.

En el ambiente demo del firewall Fortigate 2000E se identificaron configuraciones que requieren ajuste, como reglas de acceso demasiado permisivas, falta de autenticación robusta, parches pendientes, y perfiles de protección aplicados parcialmente. El análisis de riesgos permitió priorizar las acciones de remediación, enfocándose en fortalecer los controles de acceso, actualizar el firmware, implementar autenticación multifactor, mejorar la segmentación de red y asegurar el monitoreo continuo de eventos.

El plan de acción propuesto establece las prioridades críticas y las acciones necesarias para avanzar hacia un nivel de madurez adecuado, permitiendo a la organización reducir la superficie de ataque, mejorar la resiliencia operativa y cumplir con los estándares exigidos por socios internacionales.

Por útimo, la adopción de buenas prácticas como la firma de acuerdos de confidencialidad, el uso de herramientas colaborativas para la gestión de auditorías y la documentación estructurada de hallazgos y riesgos, contribuyen a una auditoría profesional y alineada con los requerimientos actuales de ciberseguridad.