UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Diseño De Un Modelo De Ciberresiliencia Para El Gad Municipal De Salcedo Basado En Inteligencia Artificial Para La Detección Temprana Y Gestión De Anomalías.

AUTOR
Ilbay Villacís, Roberto Carlos

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR
Tello Oquendo, Luis Patricio

Santa Elena, Ecuador
Año 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
LUIS PATRICIO TELLO OQUENDO

Ing. Luis Tello Oquendo, PhD.
TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
CARLOS ANDRES CASTILLO YAGUAL

Ing. Carlos Castillo Yagual, Mgtr.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
CARLOS EFRAIN SANCHEZ LEON

Ing. Carlos Sánchez León, Mgtr.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **ILBAY VILLACÍS ROBERTO CARLOS**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
LUIS PATRICIO TELLO OQUENDO

Ing. Luis Tello Oquendo, Ph.D.

Santa Elena, 30 de junio del 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **ILBAY VILLACÍS ROBERTO CARLOS**

DECLARO QUE:

El trabajo de Titulación, denominado **"DISEÑO DE UN MODELO DE CIBERRESILIENCIA PARA EL GAD MUNICIPAL DE SALCEDO BASADO EN INTELIGENCIA ARTIFICIAL PARA LA DETECCIÓN TEMPRANA Y GESTIÓN DE ANOMALÍAS"**, previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 30 de junio del 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ROBERTO CARLOS ILBAY VILLACIS

Ilbay Villacís Roberto Carlos

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **DISEÑO DE UN MODELO DE CIBERRESILIENCIA PARA EL GAD MUNICIPAL DE SALCEDO BASADO EN INTELIGENCIA ARTIFICIAL PARA LA DETECCIÓN TEMPRANA Y GESTIÓN DE ANOMALÍAS**, presentado por el estudiante **ILBAY VILLACÍS ROBERTO CARLOS** fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 9%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


Certificado de análisis
Compilatio Magister+ | UNACH-ECU

TESIS_Roberto_Ilbay_v2
ID : f4ee6ae7c1e2a43260e4bf388ee1a2f5398f869f

9%
Textos sospechosos

Nombre del fichero : TESIS_Roberto_Ilbay_v2.txt
Tamaño del archivo original : 1,02 MB
Número de palabras : 16.679

Depositante : LUIS PATRICIO TELLO OQUENDO
Fecha de depósito : 29 de junio de 2026
Tipo de carga : interface
fecha de fin de análisis : 29 de junio de 2026

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
LUIS PATRICIO TELLO OQUENDO

Ing. Luis Tello Oquendo, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **ILBAY VILLACÍS ROBERTO CARLOS**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 30 de junio del 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ROBERTO CARLOS
ILBAY VILLACIS

Ilbay Villacís Roberto Carlos

AGRADECIMIENTO

Al Instituto de Postgrado de la Universidad Estatal Península de Santa Elena, por brindar las condiciones académicas necesarias para el desarrollo de esta investigación. A los docentes del programa de Maestría en Ciberseguridad, cuya guía y aportes científicos enriquecieron cada etapa del proceso formativo. Al PhD. Luis Patricio Tello Oquendo, tutor de este trabajo, por su orientación metodológica y acompañamiento constante. A las autoridades y al equipo de Tecnologías de la Información y Comunicaciones del GAD Municipal de Salcedo, cuya apertura y colaboración hicieron posible el acceso a los datos reales y la infraestructura que sustentaron la presente investigación.

Ilbay Villacís, Roberto Carlos

DEDICATORIA

A mi familia, por su apoyo incondicional durante este proceso de formación académica. A los funcionarios del GAD Municipal de Salcedo, cuyo compromiso con la mejora continua de los servicios digitales hizo posible esta investigación. Y a todos los profesionales de ciberseguridad del sector público ecuatoriano que trabajan a diario para proteger los servicios que la ciudadanía necesita.

Ilbay Villacís, Roberto Carlos

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Antes de la intervención, la ciberseguridad del GAD Municipal de Salcedo dependía de procedimientos manuales y reactivos, con tiempos de detección de incidentes superiores a 14 horas. Para revertir esa situación, se diseñó e implementó un modelo de ciberresiliencia conforme al EGSI v3, apoyado en inteligencia artificial para la detección temprana. Los participantes fueron los siete funcionarios del equipo TIC del GAD. Con ese grupo se ejecutaron mediciones antes y después de la intervención, dentro de un esquema cuasi-experimental de enfoque mixto. La evidencia se construyó sobre 8,5 millones de eventos analizados, encuestas Likert y entrevistas. OpenSearch 2.19.5 ejecutó tres detectores Random Cut Forest aplicados a logs de firewall, correo y servidor web. Los resultados muestran que el MTTD pasó de 840 a 3 minutos y el MTTR de 1 080 a 27 minutos, con diferencias estadísticamente significativas (t de Student, p-valor < 0,05). El modelo resulta replicable en municipios que operan con presupuesto limitado.

Palabras clave: ciberresiliencia, detección de anomalías, OpenSearch.

ABSTRACT

Cybersecurity at the Municipal GAD of Salcedo previously relied on manual and reactive procedures, with incident detection times exceeding 14 hours. To address this situation, a cyber-resilience model aligned with EGSI v3 was designed and implemented, supported by artificial intelligence for early threat detection. The seven members of the municipal TIC´S team participated in the study. Pre- and post-intervention measurements were conducted using a quasi-experimental mixed-methods approach. Evidence was built from 8,5 million analyzed events, Likert-type surveys, and interviews. OpenSearch 2.19.5 executed three Random Cut Forest detectors applied to firewall, email, and web server logs. The results show that the Mean Time to Detect (MTTD) decreased from 840 to 3 minutes and the Mean Time to Respond (MTTR) from 1 080 to 27 minutes, with statistically significant differences according to Student's t-test (p-value < 0,05). The model is replicable in municipalities operating with limited budgets.

Keywords: cyber-resilience, anomaly detection, OpenSearch

LISTA DE ABREVIATURAS Y SIGLAS

Sigla	Significado
AI RMF	Artificial Intelligence Risk Management Framework (NIST)
API	Application Programming Interface
BCDR	Business Continuity and Disaster Recovery
CISA	Cybersecurity and Infrastructure Security Agency
CV	Coeficiente de Variación
DoS	Denial of Service — Denegación de Servicio
EGSI v3	Esquema Gubernamental de Seguridad de la Información
ENISA	European Union Agency for Cybersecurity
FP	Falso Positivo
GAD	Gobierno Autónomo Descentralizado
HTTP	Hypertext Transfer Protocol
IA	Inteligencia Artificial
IAM	Identity and Access Management

IEC	International Electrotechnical Commission
IMAP	Internet Message Access Protocol
INC	Incidente (identificador interno de gestión)
IPS	Intrusion Prevention System
IVC	Índice de Validez de Contenido
KPI	Key Performance Indicator
LOPDP	Ley Orgánica de Protección de Datos Personales (Ecuador)
MFA	Multi-Factor Authentication
MINTEL	Ministerio de Telecomunicaciones
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
NAS	Network Attached Storage
NIST CSF	NIST Cybersecurity Framework
PDCA	Planificar – Hacer – Verificar – Actuar

RAM	Random Access Memory
RACI	Responsible, Accountable, Consulted, Informed
RCF	Random Cut Forest
SFOS	Sophos Firewall Operating System
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SPSS	Statistical Package for the Social Sciences
TIC	Tecnologías de la Información y Comunicaciones
VM	Máquina Virtual
VPN	Red Privada Virtual
WAF	Web Application Firewall
ZTA	Zero Trust Architecture

INTRODUCCIÓN

La transformación digital en los gobiernos locales de América Latina presentó una paradoja que merece atención: mientras que la mayoría de los municipios adoptaron portales transaccionales e infraestructuras híbridas, solo un tercio contaba con sistemas de gestión de seguridad completos que ampliaban considerablemente su área de ataque (Hossain et al., 2024). En Ecuador, a pesar de las directrices del Esquema Gubernamental de Seguridad de la Información versión 3 (EGSI v3), el cumplimiento documental y la operación técnica real en los GADs aún no están alineados.

Salcedo es un cantón en Cotopaxi con aproximadamente 58,000 habitantes. Su GAD Municipal apoya los servicios públicos en una infraestructura tecnológica que ha crecido sin un modelo operativo de seguridad acompañante. Desde noviembre de 2025 hasta marzo de 2026, los registros del firewall Sophos XGS3100 registraron eventos críticos en la cantidad de 95,456 ataques IPS en 24 horas. El vector DoS tuvo una alta correlación con una inundación SMTP simultánea de 0.9991. Esto significa que había una relación muy fuerte entre estos dos eventos. En otras palabras, el vector DoS y la inundación SMTP ocurrieron de manera coordinada durante el ataque. Así que los dos comportamientos estaban muy estrechamente relacionados. La correlación de Pearson es una forma de medir la relación entre dos variables y en este caso el resultado indica que el vector DoS y la inundación SMTP estaban muy relacionados. Esto sucedió sin alerta automatizada y sin un protocolo de respuesta documentado.

El modelo desarrollado integra cuatro componentes en OpenSearch 2.19.5: capa de gobernanza con matrices RACI y runbooks; monitoreo centralizado de ocho índices que

procesaron más de 7.4 millones de documentos; tres detectores de anomalías Random Cut Forest; y un tablero de KPIs operativos en OpenSearch Dashboards.

El informe se divide en tres partes. La primera parte aborda lo que ya se sabía antes de comenzar la investigación, el problema que queríamos resolver, por qué emprendimos esta investigación y por qué era importante para nosotros realizar este estudio y cómo lo hicimos. La segunda parte toca las teorías consideradas, las reglas y cómo se recopilaron y analizaron los datos. La tercera parte es la propuesta para desarrollar la ciberresiliencia utilizando EGSI v3, cómo se implementó en el GAD Municipal de Salcedo para mostrar resultados y qué podemos aprender de ellos. Finalmente, se dan las conclusiones y recomendaciones de todo esto.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

La vulnerabilidad de los GAD ecuatorianos a las amenazas cibernéticas no es teórica. En Quito, un ataque de ransomware por parte del grupo BlackCat afectó parte de la base de datos institucional. El propio GAD de Salcedo, antes de contar con el Sophos XGS3100, ya había sufrido un incidente de ransomware sin impacto registrado y alrededor de 2018 enfrentó un ataque de spam contra su servidor web.

Hay precedentes regionales con resultados concretos. En el Municipio de Miraflores (Lima, Perú), la adopción de un monitoreo unificado articulado con matrices de responsabilidades llevó el MTTD de 187 a 48 días y el MTTR de 45 a 21 días (Grothe et al., 2021). En el plano más técnico, los modelos no supervisados tipo Random Cut Forest superan en hasta un 68% a las soluciones basadas en firmas para detectar incidentes en redes gubernamentales (CISA, 2023). La aplicación de este enfoque en municipios latinoamericanos con equipos TIC reducidos ($N \leq 10$) aún no cuenta con suficiente documentación pública.

1.2 DESCRIPCIÓN DEL PROYECTO

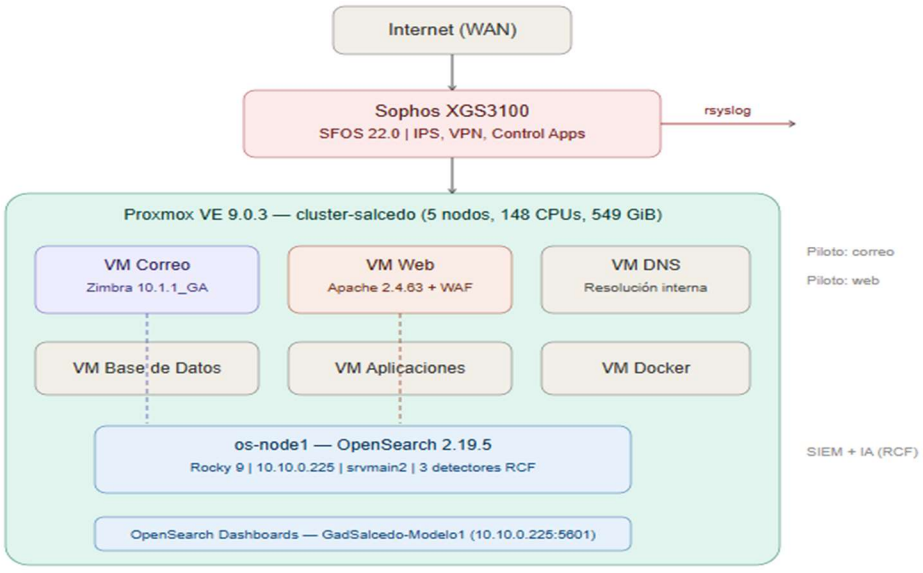
El objetivo del proyecto fue diseñar e implementar un modelo operativo de ciberresiliencia para el GAD Municipal de Salcedo. Toda la propuesta se montó sobre infraestructura ya existente en el municipio. Esa base la conforman el firewall `Sophos XGS3100`, el hipervisor Proxmox VE 9.0.3 que organiza el clúster `cluster-salcedo` de cinco nodos (148 CPUs, 549 GiB RAM y un NAS de 42 TB) y las 20 máquinas virtuales actualmente en producción. Sobre ese stack se

incorporó OpenSearch 2.19.5 como pieza central, instalado en una VM Rocky Linux 9 (`os-node1, IP 10.10.0.225`) en el nodo `srvmain2`.

La pila de tecnología se implementó de la siguiente manera: Sophos XGS3100 → rsyslog → scripts de normalización en Python → OpenSearch 2.19.5 → OpenSearch Dashboards. Se crearon ocho índices de datos: Sophos-firewall (8,305,135 documentos, 2.5 GB), `apache-access` (137,325 documentos), `apache-error` (8,265 documentos), `apache-modsec` (50,470 documentos), `zimbra-mail` (16,110 documentos), `zimbra-audit` (796 documentos), `zimbra-nginx` (5,225 documentos) y `gad-incidents` (5 documentos). Se utilizaron tres detectores Random Cut Forest para cada servicio crítico: el firewall, el servidor web (Apache 2.4.63 con ModSecurity WAF en Rocky Linux 10) y el servidor de correo (Zimbra 10.1.1_GA en Rocky Linux 9.6). La Figura 1 muestra la tecnología de GAD Salcedo con los componentes piloto y el flujo de datos desde Sophos XGS3100 hasta OpenSearch 2.19.5.

Figura 1.

Diagrama de infraestructura tecnológica del GAD Salcedo



Nota. Elaboración propia. Arquitectura del entorno piloto con Sophos XGS3100, clúster Proxmox y servicios virtualizados.

El marco normativo integró el EGSI v3 como referente nacional, el NIST CSF 2.0 como marco de funciones de seguridad, la ISO/IEC 27001:2022 como estándar internacional, el NIST AI RMF 1.0 para el gobierno del modelo de IA, y la LOPDP para la protección de datos personales.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Diseñar e implementar un modelo operativo de gobernanza y ciberresiliencia para el GAD Municipal de Salcedo, alineado con el EGSI v3, que integre procesos, roles definidos y un sistema de KPIs operativos basado en OpenSearch con Random Cut Forest, para fortalecer la detección y respuesta ante incidentes y garantizar la continuidad de los servicios digitales.

1.3.2 OBJETIVOS ESPECÍFICOS

- Diagnosticar la madurez de seguridad del GAD Salcedo mediante el EGSI v3, identificando brechas en controles técnicos y estableciendo métricas base MTTD y MTTR en los servicios de correo electrónico y servidor web.
- Diseñar el modelo operativo que integre políticas, procesos, matriz RACI y sistema de KPIs alineados al EGSI v3 y NIST CSF 2.0.
- Desplegar un piloto de detección de incidentes en los servicios críticos del GAD apoyado en OpenSearch y detectores Random Cut Forest.
- Comparar métricas antes y después de la implementación y reportar las lecciones aprendidas.

1.4 JUSTIFICACIÓN DEL PROYECTO

Las reglas de evidencia descartan cualquier enfoque manual. Los ataques diarios de IPS del GAD Salcedo mostraron un Coeficiente de Variación de 1,645% y una correlación r = 0,9991 entre los vectores IPS y SMTP, con un pico de 95,456 ataques, 29,546 veces el promedio diario histórico del sistema. El marco regulatorio lo hace más urgente: EGSI v3 estipula medidas de rendimiento, comités activos y evidencia de cumplimiento (MINTEL, 2024a), mientras que el diagnóstico interno mostró una madurez promedio de 1,0 sobre 5 y tres dominios en un nivel inexistente. El proyecto deja un modelo para otros GAD ecuatorianos y se basa en infraestructura existente y herramientas de código abierto.

1.5 ALCANCE DEL PROYECTO

El trabajo abarcó dos servicios digitales clave de GAD Salcedo. El primero es el servidor de correo electrónico (Zimbra 10.1.1_GA, IP 10.10.0.192). El segundo es el servidor web (Apache 2.4.63 con ModSecurity WAF). La implementación se completó en cuatro etapas del proyecto preliminar:

- Diagnóstico y línea base: enero - febrero 2026.
- Diseño del modelo: febrero - marzo 2026.
- Despliegue piloto con OpenSearch y tres detectores RCF: semana 3 de marzo 2026.
- Evaluación comparativa pre/post: semana 4 de marzo 2026.

Los datos de Sophos se recopilan continuamente desde noviembre 2025 hasta marzo 2026.

CAPÍTULO II

2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO TEÓRICO

El marco teórico está compuesto por cuatro pilares: la gobernanza de la seguridad de la información en el sector público ecuatoriano, la ciberresiliencia como una mejora sobre el enfoque reactivo, la detección de anomalías mediante aprendizaje no supervisado y las métricas operativas que cuantifican los controles. La revisión de estos pilares proporciona soporte técnico para el diseño propuesto y articula los requisitos de EGSI v3, las prácticas de NIST CSF 2.0 e ISO/IEC 27001:2022 con el algoritmo Random Cut Forest implementado en OpenSearch 2.19.5. Cada pilar se desarrolla en las siguientes secciones.

2.1.1 Gobernanza y Marcos Normativos

El EGSI v3 tiene cinco niveles de madurez que van desde 0 (inexistente) hasta 5 (optimizado) en las etapas inicial, repetible, definida y gestionada. Para llegar a ese nivel, es necesario desarrollar un Proyecto de Implementación de Seguridad Institucional (ISIP): comité activo y partes responsables, indicadores monitoreados y verificables (MINTEL, 2024a). En paralelo, el NIST CSF 2.0 tiene seis funciones de seguridad: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar (Instituto Nacional de Estándares y Tecnología, 2024). ISO/IEC 27001:2022 define el estándar de sistemas de gestión basados en riesgos. Zero Trust se basa en el hecho de que ninguna entidad es confiable por defecto, y los registros indican intentos de acceso no autorizados dentro de la red (Rose et al., 2020).

2.1.2 Ciberresiliencia y Gestión de Incidentes.

La resiliencia cibernética es más que solo ciberseguridad. Permite anticipar, absorber, recuperarse y adaptarse ante incidentes sin interrupción de las operaciones (Agencia de la Unión Europea para la Ciberseguridad, 2024). El contexto municipal latinoamericano lo dificulta: presupuestos bajos, personal limitado y alta rotación de personal impiden la adopción de modelos de seguridad robustos (Hossain et al., 2024). Los números lo respaldan. Los gobiernos locales reportan un MTTD de 187 días y un MTTR de 45 días, lo cual es diez veces más alto que el estándar internacional, que requiere un MTTD de menos de 24 horas para incidentes críticos.

2.1.3 Random Cut Forest para Detección de Anomalías.

OpenSearch introduce Random Cut Forest como un detector nativo. El algoritmo crea árboles de cortes aleatorios sobre los datos y los datos atípicos se aíslan con menos cortes y, por lo tanto, reciben puntuaciones de anomalía más altas. Se adapta al contexto de GAD Salcedo de tres maneras: no requiere datos etiquetados ya que es un aprendizaje no supervisado, funciona en streaming y no asume una distribución normal (Iturbe-Araya et al., 2025). Los cinco parámetros fueron `number_of_trees` (implícito), `shingle_size` (8), `history` (40), `detection_interval` (1 minuto) y suppression rules `IGNORE_ANOMALY` con una proporción ≤ 0,2 para reducir falsos positivos.

Para gestionar los riesgos asociados al modelo durante su ciclo de vida, se abordaron aspectos como sesgos, privacidad y transparencia siguiendo las directrices del NIST AI RMF 1.0 (Instituto Nacional de Estándares y Tecnología, 2023). La gobernanza operativa se llevó a cabo a través de tres prácticas: reentrenamiento mensual, validación de umbrales y evaluación trimestral del rendimiento.

2.1.4 Métricas Operativas

Para gestionar los riesgos asociados al modelo durante su ciclo de vida, se abordaron aspectos como sesgos, privacidad y transparencia siguiendo las directrices del NIST AI RMF 1.0 (Instituto Nacional de Estándares y Tecnología, 2023). La gobernanza operativa se llevó a cabo a través de tres prácticas: reentrenamiento mensual, validación de umbrales y evaluación trimestral del rendimiento.

2.1.5 Marco conceptual

La resiliencia cibernética es la capacidad de una organización para anticipar, resistir, recuperarse y adaptarse a condiciones adversas, ataques y/o brechas en sistemas que dependen de recursos cibernéticos (Instituto Nacional de Estándares y Tecnología, 2024). La ciberseguridad tradicional se basa en prevenir el acceso no autorizado. La resiliencia cibernética asume que los incidentes ocurrirán y que la empresa es capaz de mantener la operación durante y después del evento. Por eso fue tan importante el GAD Municipal de Salcedo. Con los recursos que teníamos a nuestra disposición era imposible tener un perímetro impenetrable; lo que era posible era reducir los tiempos de detección y coordinar una respuesta.

Un SIEM centraliza la gestión de registros en un solo lugar. Sus tareas son cuatro: recopilar, normalizar, almacenar y analizar registros de diferentes fuentes. En GAD Salcedo, esto se realiza mediante OpenSearch 2.19.5, que unifica los registros del firewall Sophos XGS3100, el servidor web Apache con ModSecurity y el servidor de correo Zimbra; en este repositorio único, se llevan a cabo la búsqueda, la correlación y la visualización en tiempo real.

Una anomalía es un comportamiento que es diferente de lo que se considera normal. Detectarla, en la práctica, es poder reconocer esa desviación con una buena significancia

estadística. En ciberseguridad, las pistas pueden ser diversas: denegación de servicio, intentos de fuerza bruta, exfiltración de datos y malware. El enfoque no supervisado se utilizó aquí en esta investigación a través del algoritmo Random Cut Forest, que no requiere mostrar datos que hayan sido previamente etiquetados como maliciosos o benignos, lo que lo hace efectivo en situaciones como GAD Salcedo, donde no había un historial clasificado de los incidentes.

El proceso implica crear múltiples árboles de decisión cortando aleatoriamente las dimensiones del espacio de datos. Dado que los valores atípicos se encuentran en áreas de baja densidad, se necesitan pocos cortes para diferenciarlos, por lo que a los valores atípicos se les otorgan puntuaciones altas. Para OpenSearch, este algoritmo es parte del complemento de detección de anomalías y no necesita herramientas adicionales.

Para evaluar un sistema de detección y respuesta ante incidentes, las métricas clave son dos: MTTD y MTTR. El MTTD, tiempo medio de detección, cuenta los minutos (u horas) entre que un evento de seguridad ocurre y el equipo lo identifica. El MTTR, tiempo medio de respuesta, cuenta los minutos entre esa identificación y la contención o resolución del incidente. Si ambas métricas bajan, el impacto operativo de los incidentes baja con ellas.

La autenticación multifactor (MFA, por sus siglas en inglés) es un control de acceso que solo permite la entrada después de verificar la identidad con al menos dos factores independientes. Los tres tipos clásicos son algo que el usuario sabe (la contraseña), algo que posee (un token o dispositivo móvil) y algo que es (biometría). Ha reducido drásticamente los ataques de fuerza bruta y el robo de credenciales, ya que un solo factor no es suficiente para obtener acceso.

La Matriz RACI es una herramienta de gestión organizacional que asigna cuatro niveles de participación a los actores involucrados en cada proceso: Responsable (quien ejecuta la tarea),

Accountable (quien rinde cuentas por el resultado), Consultado (quien aporta información antes de la decisión) e Informado (quien recibe notificación del resultado). En el modelo propuesto, esta matriz distribuyó las responsabilidades de monitoreo, respuesta y mantenimiento del sistema de detección entre los siete funcionarios del equipo TIC conforme a sus perfiles y competencias.

2.1.6 Marco Referencial

Revisar la investigación previa nos permitió identificar las experiencias en la implementación de modelos de seguridad y detección de anomalías en instituciones públicas con énfasis en los gobiernos locales de América Latina y contextos con restricciones presupuestarias similares a las del GAD Municipal de Salcedo.

Hossain et al. (2024) revisaron la situación de la ciberseguridad en los gobiernos locales a nivel mundial y concluyeron que en los países en desarrollo es menos del 2% del presupuesto total de TIC en comparación con el 10% al 15% recomendado por los estándares internacionales. Los autores afirmaron que los factores clave de vulnerabilidad incluyen un bajo número de equipos de TIC que realizan funciones de seguridad como tareas de segundo nivel y la falta de métricas operativas y herramientas perimetrales que no se conectan. El diagnóstico del GAD de Salcedo confirmó claramente estos tres criterios, por lo que es una buena representación del caso.

En su estudio sobre los gobiernos locales en América Latina, Grothe et al. (2021) midieron el impacto de los marcos de ciberseguridad, que tuvieron los municipios cuya monitorización unificada con matrices de responsabilidad mejoró su MTTD de 187 días a 48 días y su MTTR de 45 a 21 días. Citaron tres razones que contribuyeron a este éxito: la presencia de la alta dirección, la formalización de roles y responsabilidades, y el monitoreo continuo de su desempeño en

indicadores operativos. Estos mismos factores se transfirieron al modelo GAD Salcedo a través del Comité de Seguridad de TIC, la Matriz RACI y el panel de KPI en OpenSearch Dashboards.

Sobre series temporales de tráfico de red, Iturbe-Araya et al. (2025) compararon el rendimiento de varios algoritmos no supervisados para detectar ciberataques. Los autores compararon Random Cut Forest, Isolation Forest y autoencoders, y concluyeron que Random Cut Forest presentó el mejor equilibrio entre tasa de detección y control de falsos positivos en entornos con distribuciones de datos altamente sesgadas. Esta característica resultó determinante para la selección del algoritmo en el GAD Salcedo, donde la distribución de ataques IPS diarios exhibió un coeficiente de variación del 1,645% con un pico de 95 456 ataques frente a una media normal de 3,2 ataques por día.

Lu et al. (2023) investigaron técnicas de detección de anomalías en flujos de datos continuos y demostraron que los modelos basados en árboles de aislamiento con un mecanismo de ventana deslizante superan a los estáticos en la detección de anomalías contextuales (es decir, solo anómalas en el momento en que ocurren). El valor del tamaño de la teja del Bosque de Corte Aleatorio en OpenSearch implementó este mecanismo al tener en cuenta una ventana de observaciones consecutivas para cada evaluación de anomalía. El valor del tamaño de la teja de 8 en los detectores GAD Salcedo proporcionó una oportunidad para capturar correlaciones temporales que un análisis punto por punto no habría identificado.

Cinco pilares sustentan el modelo: identidad, dispositivos, redes, aplicaciones y datos, y cada uno se evalúa en tres niveles de madurez. Aunque el GAD Salcedo no tenía una arquitectura de Confianza Cero completa, sí contaba con dos de sus principios fundamentales. El primero es el

MFA en todas las cuentas del equipo de TIC. El segundo es la centralización de registros que proporciona visibilidad completa del tráfico de red independientemente de su origen.

Según el informe ENISA Threat Landscape 2024, de la Agencia de la Unión Europea para la Ciberseguridad, los ataques contra instituciones gubernamentales crecieron un 35% frente al año anterior, con ransomware y denegación de servicio a la cabeza (European Union Agency for Cybersecurity, 2024). El dato es europeo, pero la tendencia llegó también al sector público ecuatoriano. Quito sufrió un ataque de ransomware del grupo BlackCat que comprometió buena parte de su base de datos institucional, y el GAD Salcedo enfrentó el ataque coordinado de marzo de 2026 con 95 456 eventos IPS.

La guía NIST SP 1800-35 sobre arquitectura Zero Trust (Borchert et al., 2025) ofrece lineamientos prácticos para organizaciones con recursos acotados. Su recomendación principal es ir por fases: empezar por los servicios más críticos y avanzar progresivamente, en lugar de intentar una transformación integral. El piloto del GAD Salcedo aplicó esa lógica al concentrarse en los dos servicios más críticos correo electrónico y servidor web con un plan de extensión documentado para los demás.

La investigación sobre ciberseguridad en los GAD municipales en Ecuador es escasa. La mayoría de los estudios se han realizado en el gobierno central o en el sector financiero y sus hallazgos no son aplicables al contexto municipal. Nuestro trabajo busca llenar ese vacío y, al hacerlo, proporciona datos reales y métricas verificables para la implementación de un modelo de ciberresiliencia basado en inteligencia artificial en un municipio local ecuatoriano con personal de TI y presupuesto limitados.

2.1.7 Marco Legal

Tres bloques regulatorios ecuatorianos subyacen al marco legal del trabajo: seguridad de la información, protección de datos personales y gobierno electrónico. También existen estándares internacionales que el sector público ecuatoriano utiliza como referencia en esta área.

En el inciso 19 del artículo 66, la Constitución de la República del Ecuador (2008) reconoce el derecho a la protección de los datos personales. Para el propósito de este derecho, se considera el acceso a dichos datos y la decisión sobre su procesamiento, y la protección de los datos es determinada por su propietario. Esta disposición constitucional es relevante para la obligación del GAD Municipal de Salcedo y fue la base para los controles técnicos y organizativos que protegen la información personal de los ciudadanos que interactúan con los servicios digitales municipales.

El Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD, 2010) establece en los artículos 54 y 55 las competencias de los gobiernos autónomos descentralizados municipales, entre ellas, la provisión de servicios públicos. La continuidad de los servicios digitales del GAD Salcedo, incluyendo el correo electrónico institucional, el portal web y los sistemas administrativos internos, es una obligación funcional que no puede ser interrumpida y se espera que la institución cumpla con sus competencias constitucionales. El modelo de ciberresiliencia fue introducido para ayudar a garantizar la continuidad.

La Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial Suplemento 459 del 26 de mayo de 2021, y su Reglamento General publicado el 13 de noviembre de 2023, establecieron el marco de obligaciones para el tratamiento de datos personales en instituciones públicas y privadas del Ecuador. Los principios de minimización de datos (artículo 10), limitación del propósito (artículo 8), exactitud (artículo 11) y seguridad del tratamiento

(artículo 37) resultaron directamente aplicables al modelo implementado en el GAD Salcedo, dado que el sistema de monitoreo procesa logs que pueden contener información personal de ciudadanos y funcionarios. El modelo incorporó cuatro salvaguardas conforme a la LOPDP: seudonimización de IPs internas en representaciones públicas, limitación del propósito a la detección de anomalías de seguridad, acceso basado en roles y retención limitada a 12 meses conforme a los requerimientos de auditoría del EGSI v3.

La regulación requiere un Proyecto de Implementación de Seguridad Institucional. Este proyecto necesita cinco componentes mínimos: un comité de seguridad con reuniones documentadas, un oficial de seguridad con funciones formales, un inventario clasificado de activos, controles técnicos y administrativos por dominio, y evidencia verificable de progreso. La directiva MINTEL (2024b) ofrece guías operativas para poner todo esto en práctica. En el GAD Salcedo, el diagnóstico mostró una madurez promedio de 1.0 sobre 5 en los dominios evaluados, una clara brecha entre lo que exige la regulación y el funcionamiento real de la institución.

El artículo 79 de la Ley Orgánica de Telecomunicaciones (2015) obliga a las y los prestadores de servicios de telecomunicaciones a adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red y en la prestación de sus servicios.

El Código Orgánico Integral Penal (COIP, 2014) tipifica en sus artículos 229 al 234 los delitos informáticos, que incluyen la revelación ilegal de bases de datos (artículo 229), la interceptación ilegal de datos (artículo 230), la transferencia electrónica de activo patrimonial (artículo 231), el ataque a la integridad de sistemas informáticos (artículo 232), los delitos contra la información pública reservada (artículo 233) y el acceso no consentido a un sistema informático

(artículo 234). La documentación de los incidentes INC-001 a INC-004 en el índice `gad-incidentes` de OpenSearch proporciona evidencia técnica con timestamps verificables que puede servir como insumo para procesos administrativos o penales en caso de que los ataques registrados ameriten acción legal.

El Marco de Gestión de Riesgos de IA 1.0 del NIST (Instituto Nacional de Estándares y Tecnología, 2023) establece las pautas para gestionar los riesgos a lo largo del ciclo de vida del modelo de inteligencia artificial: desviación debido a cambios en los patrones de datos, sesgos algorítmicos y riesgos de privacidad. Mientras tanto, la arquitectura de Confianza Cero en NIST SP 800-207 (Rose et al., 2020) proporciona el principio de verificación continua, que en este trabajo se implementó a través de dos controles: habilitar MFA y centralizar los registros.

2.2 METODOLOGÍA DEL PROYECTO

El estudio se llevó a cabo en el GAD Municipal del Cantón Salcedo en la Provincia de Cotopaxi, Ecuador. La infraestructura utilizada consta de un firewall Sophos XGS3100 (SFOS 22.0.0 GA-Build411, serie X31006Y9MCD2F22) y un clúster Proxmox VE 9.0.3 de cinco nodos, `srvmain1` a `srvmain5`, con IPs 10.10.0.220, 10.10.0.221, 10.10.0.198, 10.10.0.5 y 10.10.0.199. Cuenta con 148 CPUs, 549 GiB de RAM y 63.64 TiB de almacenamiento, que se complementa con un NAS de 42 TB (`srvnas0`). En total, 20 máquinas virtuales están trabajando en producción en una red de datos local con conexión VPN. El equipo de TI estaba compuesto por 7 empleados: el gerente de TI (Ing. Roberto Ilbay), tres técnicos generalistas y tres empleados administrativos.

2.2.1 Metodología de investigación

La investigación se enmarcó en el paradigma pragmático, dado que combinó técnicas cuantitativas y cualitativas para abordar un problema práctico de seguridad de la información en

el sector público. El tipo de investigación fue aplicada, orientada a resolver la ausencia de capacidades de detección automatizada en el GAD Municipal de Salcedo mediante el diseño e implementación de un modelo operativo verificable con datos reales. Por su alcance, la investigación fue descriptiva en la fase de diagnóstico, al caracterizar el estado de madurez del EGSI v3, y explicativa en la fase de evaluación, al demostrar la relación causal entre la implementación del modelo y la reducción de los tiempos MTTD y MTTR.

2.2.2 Técnicas de recolección de información

Había cuatro métodos complementarios en marcha. La encuesta estructurada con un cuestionario de 25 ítems con escala Likert en seis subescalas, medía el nivel de madurez en seguridad de la información del equipo de TI. La entrevista semiestructurada se dividió en cuatro bloques temáticos, que se utilizaron para obtener percepciones cualitativas de los siete funcionarios sobre los controles actuales, experiencias de incidentes y expectativas del modelo adoptado. La observación in situ nos permitió verificar la configuración del equipo, los controles técnicos y el estado de la documentación de seguridad. El análisis de documentos y registros cubrió tres direcciones: políticas de seguridad actuales e historial de incidentes, y la extracción automática de telemetría del Sophos XGS3100 a través de rsyslog y scripts de Python. Esta extracción se alimentó en los ocho índices de OpenSearch que en conjunto han registrado casi 8.5 millones de eventos.

El enfoque del estudio fue mixto y combinó dos componentes en paralelo. El componente cuantitativo se centró en tres frentes: el análisis estadístico de los logs del firewall (media, mediana, desviación estándar y correlación de Pearson), la comparación pre/post de MTTD y MTTR mediante prueba t de Student para muestras pareadas, y la evaluación de la confiabilidad del instrumento con Alfa de Cronbach. El componente cualitativo trabajó con análisis temático inductivo sobre las entrevistas semiestructuradas aplicadas a los siete funcionarios del equipo TIC;

la codificación arrojó cuatro temas principales: percepción de vulnerabilidad institucional, barreras organizacionales, confianza en la tecnología existente y expectativas del modelo. Al cruzar ambos componentes, la triangulación entregó evidencia convergente y reforzó la validez de los resultados.

2.2.3 Diseño de investigación

Este estudio fue cuasi-experimental, pretest/posttest con una sola muestra (O_1 X O) donde O_1 es la medición de referencia antes de la intervención, X es el piloto con OpenSearch y detectores RCF, y O es la medición subsiguiente para mostrar cambios en indicadores como MTTD, MTTR y volumen de ataque. Como tipo de investigación, mi tipo fue mixto: la parte cuantitativa es operativa y la parte cualitativa son las percepciones del equipo de TI recogidas en entrevistas semiestructuradas. La población consistió en todo el equipo de TI (N = 7). Los datos se recopilaron como encuestas estructuradas tipo Likert con 25 ítems en seis subescalas, extracción automática de telemetría de Sophos y formularios de registro de incidentes. La calidad fue evaluada por juicio de expertos (IVC $\geq$ 0.80) y la fiabilidad por el Alfa de Cronbach (α = 0.83). Los datos fueron analizados con SPSS Statistics, Excel y Python (NumPy/Pandas/SciPy).

2.2.4 Grupos poblacionales involucrados

La población de estudio consistió en el equipo de Tecnologías de la Información y Comunicación del GAD Municipal de Salcedo, compuesto por siete funcionarios: el jefe de TIC (Ing. Roberto Ilbay), tres técnicos generalistas en el rol de administración de redes, sistemas y soporte, y tres funcionarios administrativos en los sistemas institucionales. Debido a la pequeña población, se utilizó un censo total (N = 7) sin muestreo para asegurar la cobertura completa de los actores involucrados en los procesos de seguridad de la información. Esto se hizo porque los siete funcionarios son los únicos con acceso privilegiado a la infraestructura tecnológica y, por lo tanto, los actores en el modelo de ciberresiliencia propuesto.

2.2.5 Procedimiento para la recolección y análisis de datos

El procedimiento se ejecutó en cuatro etapas secuenciales alineadas con las fases del anteproyecto. En la primera etapa se aplicaron las encuestas estructuradas tipo Likert y las entrevistas semiestructuradas a los siete funcionarios, se realizó la revisión documental de las políticas existentes y se ejecutó la evaluación de madurez EGSI v3 mediante observación directa. En la segunda etapa se configuró la infraestructura de monitoreo: el envío de logs del Sophos vía rsyslog, los pipelines de ingesta Python para Apache y Zimbra, y los ocho índices en OpenSearch. En la tercera etapa se activaron los tres detectores Random Cut Forest, se configuraron los monitores de alertas por correo electrónico y se habilitó la MFA en las siete cuentas del equipo TIC. En la cuarta etapa se recolectaron las métricas post-implementación a partir de los cuatro incidentes gestionados (INC-001 a INC-004), se calcularon los indicadores MTTD y MTTR, y se ejecutaron los análisis estadísticos en SPSS: prueba t de Student pareada para la comparación pre/post, correlación de Pearson para la relación entre vectores de ataque, y Alfa de Cronbach para verificar la confiabilidad del instrumento.

2.2.6 Variables de la Investigación

La investigación operó con una variable independiente y cinco variables dependientes que permitieron medir el efecto de la intervención sobre la capacidad de detección y respuesta del GAD Municipal de Salcedo.

La variable independiente fue el modelo de ciberresiliencia basado en inteligencia artificial, operacionalizada como el conjunto integrado de componentes de gobernanza, monitoreo, detección con Random Cut Forest y evaluación continua implementados sobre la plataforma OpenSearch 2.19.5. Su nivel de implementación se midió mediante la rúbrica de madurez del EGSI v3 en escala de 0 a 5 y las subescalas Likert del cuestionario aplicado al equipo TIC.

Las variables dependientes fueron cinco. El MTTD, expresado en minutos, midió el intervalo promedio entre la ocurrencia de un evento de seguridad y su detección, calculado como la sumatoria de las diferencias entre el tiempo de detección y el tiempo de ocurrencia dividida entre el número de incidentes. El MTTR, también expresado en minutos, midió el intervalo promedio entre la detección y la resolución del incidente con la misma lógica de cálculo. La disponibilidad de los servicios se expresó como el porcentaje de tiempo operativo respecto al tiempo total programado. El porcentaje de MFA habilitada midió la proporción de cuentas con autenticación multifactor activa respecto al total de cuentas del equipo TIC. La tasa de falsos positivos del modelo de IA midió la proporción de alertas incorrectas respecto al total de alertas generadas por los detectores RCF.

Tabla 1.

Variables de Investigación — Modelo de Ciberresiliencia GAD Salcedo

Tipo	Variable	Unidad	Forma de Medición
Independiente	Modelo de ciberresiliencia basado en IA	Nivel 0–5	Rúbrica EGSI v3 + subescalas Likert
Dependiente	MTTD	Minutos	Σ(t_detección – t_ocurrencia) / N incidentes
Dependiente	MTTR	Minutos	Σ(t_respuesta – t_detección) / N incidentes
Dependiente	Disponibilidad servicios	Porcentaje	(Tiempo operación / Tiempo total) × 100
Dependiente	MFA habilitada	Porcentaje	(Cuentas MFA / Total cuentas) × 100

Dependiente	Tasa FP del modelo IA	Porcentaje	(Alertas FP / Total alertas) × 100

Nota. Elaboración propia con base en EGSI v3 (MINTEL, 2024a) y NIST CSF 2.0.

CAPÍTULO III

3. PROPUESTA – MODELO DE CIBERRESILIENCIA

La elección del GAD Municipal de Salcedo como caso de estudio respondió a dos criterios: conveniencia operativa y relevancia científica. Salcedo es un cantón de la provincia de Cotopaxi situado 35 kilómetros al sur de Latacunga, con coordenadas 1°03'28"S, 78°35'24"W y una altitud de 2.683 m.s.n.m.; cuenta con cerca de 58.000 habitantes repartidos en seis parroquias. El GAD ofrece servicios digitales como recaudación en línea, trámites municipales, gestión documental interna, correo electrónico institucional y portal web informativo. La interrupción de cualquiera de ellos compromete la capacidad institucional para cumplir sus funciones constitucionales.

3.1 Diagnóstico de la Insfrestructura

3.1.1 Volumen de Telemetría Indexada

La Tabla 2 presenta el volumen de datos reales indexados en OpenSearch 2.19.5, que constituyeron la base empírica del modelo de detección.

Tabla 2.

Volumen de Telemetría por Índice en OpenSearch — GAD Salcedo

Índice	Documentos	Tamaño	Fuente / Servicio
sophos-firewall	8 305,135	2,5 GB	Firewall perimetral Sophos XGS3100
apache-access	137 325	17,6 MB	Servidor web Apache 2.4.63
apache-modsec	50 470	8,0 MB	WAF ModSecurity — servidor web
apache-error	8 265	2,2 MB	Errores del servidor web

zimbra-mail	16 110	3,5 MB	Servidor correo Zimbra 10.1.1_GA
zimbra-nginx	5 225	725 KB	Proxy Nginx — correo
zimbra-audit	796	551 KB	Auditoría de correo
gad-incidentes	5	20,9 KB	Registro de incidentes del modelo
TOTAL	8 523,331	~2,53 GB	3 fuentes + registro de incidentes

Nota. Datos consultados el 26 de marzo de 2026 mediante API REST de OpenSearch. El índice sophos-firewall acumula logs desde noviembre de 2025.

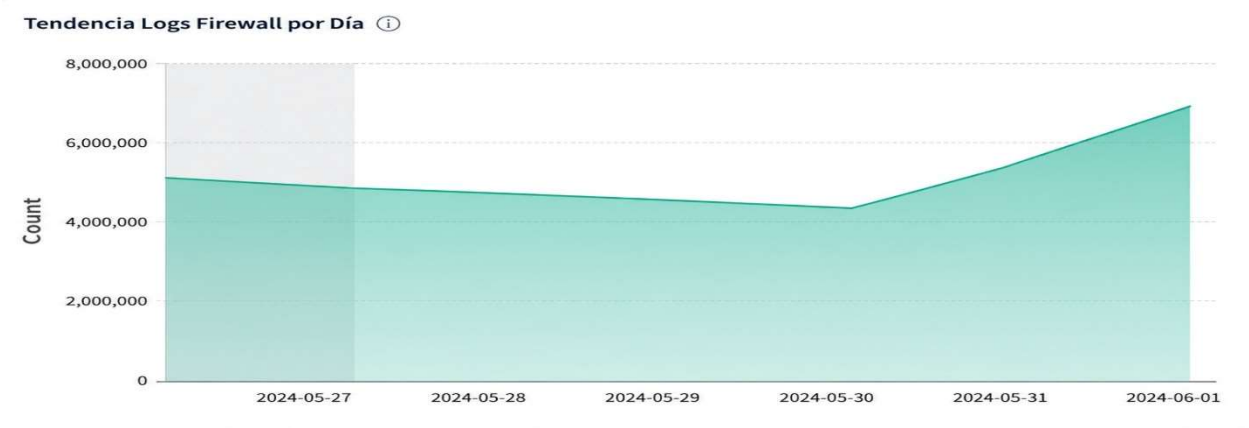
3.1.2 Análisis de Logs del Firewall

Descubrimos que en un lapso de 8.3 millones de eventos entre noviembre de 2025 y marzo de 2026, el índice de `sophos-firewall` acumuló 8.3 millones de ataques. El comportamiento temporal fue muy bimodal. La línea base fue muy baja, entre 1 a 6 ataques IPS por día, y en marzo de 2026 hubo una ventana de 48 horas que concentró 95,456 ataques en un solo día. Esto se debió a un ataque DoS simultáneo al servicio de respaldo Veritas y una inundación SMTP simultánea; la correlación entre ambos vectores fue casi perfecta (Pearson $r = 0{,}9991$, $p < 0{,}001$). En esta ventana, la IP maliciosa 185.218.138.11, que se encontró como fuente de escaneo y fuerza bruta, realizó 6 intentos contra el puerto 4443 y tres fallos de autenticación VPN en 3 segundos.

La Figura 2 muestra la tendencia de los registros del firewall por día.

Figura 2.

Tendencia de logs de firewall por día (noviembre 2025 – marzo 2026)



Nota. Datos extraídos del índice `sophos-firewall` en OpenSearch 2.19.5.

Tabla 3.

Estadística Descriptiva — Ataques IPS Diarios

Métrica	Valor	Interpretación
Media diaria — días normales (μ_n)	3,2 ataques/día	Línea base para el modelo RCF
Mediana	3 ataques/día	Comportamiento típico en valores bajos
Desviación estándar total (σ)	119 642	Alta dispersión por eventos extremos
Coeficiente de Variación (CV)	1,645%	Gestión manual inviable
Umbral advertencia ($\mu_n+1\sigma_n$)	≈ 26 ataques/día	Notificación al equipo TIC
Umbral crítico ($\mu_n+2\sigma_n$)	≈ 49 ataques/día	Protocolo de respuesta inmediata
Correlación Pearson IPS–SMTP	r = 0,9991	Ataque coordinado confirmado
Pico máximo	95 456 ataques/24h	29.546× la media normal

Nota. Cálculos con Python (NumPy/Pandas/SciPy) y verificados en SPSS Statistics sobre los datos del Sophos XGS3100.

3.1.3 Análisis del Servidor Web y Correo.

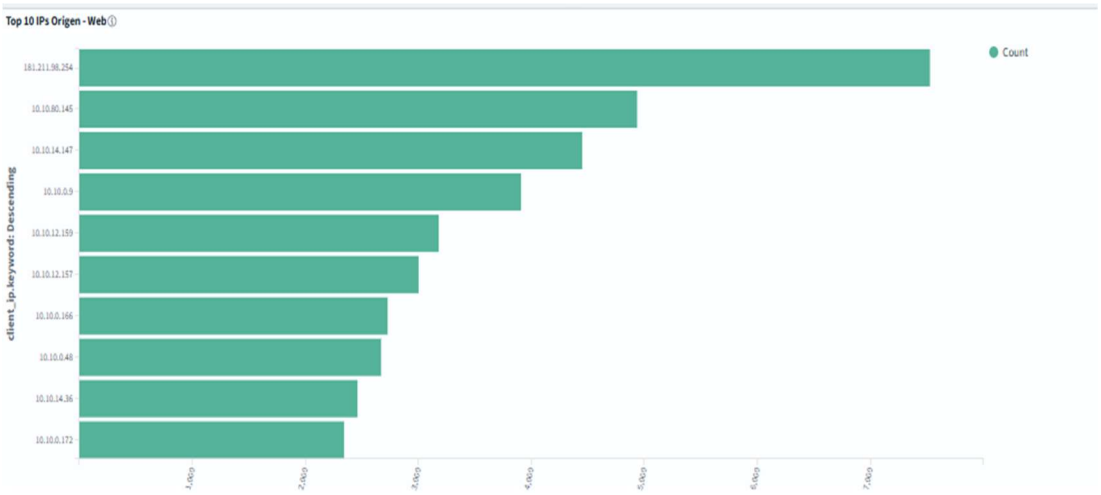
El servidor web Apache tuvo 137,325 accesos, 50,470 eventos de ModSecurity WAF y 8,265 errores durante el tiempo que examinamos. Los métodos HTTP más comunes fueron GET, POST, PUT, DELETE y PROPFIND, con códigos de respuesta 200, 304, 408, 201 y 404. La IP más activa fue 181.211.36.254, seguida por tráfico interno de IPs en el rango 10.10.x.x. INC-003 (de alta severidad) fue identificado como tráfico WAF anómalo detectado por el detector Apache-ModSec en 5 minutos.

El servidor de correo Zimbra tuvo 16,110 eventos de operación, 5,225 eventos de proxy Nginx y 796 registros de auditoría. Los usuarios más activos fueron rilbay@salcedo.gob.ec, enrique.arcos@salcedo.gob.ec y tecnologia@salcedo.gob.ec. Los principales niveles de registro fueron imap, soap, account, purge y FileUploadServlet. Durante este tiempo, Zimbra tuvo 1,225 fallos de autenticación y esto hizo que MFA fuera un parámetro de objetivo prioritario del modelo.

La Figura 3 muestra las diez IPs principales con el mayor número de solicitudes al servidor web. 181.211.36.254 es la dirección externa más activa.

Figura 3.

Top 10 IPs origen — servidor web del GAD Salcedo



Nota. Datos extraídos del índice apache-access en OpenSearch 2.19.5.

3.1.4 Evaluación de Madurez EGSI v3.

Tabla 4.

Evaluación de Madurez EGSI v3 — GAD Municipal de Salcedo (Pre-implementación)

Dominio EGSI v3	Nivel (0–5)	Meta	Brecha
Comité y gobernanza de seguridad	0 — Inexistente	3	Sin comité, reuniones ni actas
Política de seguridad	1 — Inicial	3	Documento sin comunicar ni operacionalizar
Gestión de activos	2 — Repetible	3	Inventario parcial sin clasificación
Control de acceso (IAM)	1 — Inicial	3	Sin MFA, sin revisión de privilegios
Monitoreo y logs	2 — Repetible	4	Sin correlación automática ni alertas
Respuesta ante incidentes	0 — Inexistente	3	Sin runbooks ni tiempos definidos
Continuidad del servicio	2 — Repetible	3	Backups sin pruebas de restauración

Gestión de vulnerabilidades	1 — Inicial	3	Sin parchado periódico ni escaneos
Medición de KPIs	0 — Inexistente	3	Sin indicadores formales
PROMEDIO	1,0 / 5	3,1 / 5	Brecha de 2,1 niveles

Nota. Evaluación mediante entrevistas, revisión documental y observación directa. Escala EGSI v3**.**

3.1.5 Resultados de la Encuesta de Madurez

Tabla 5.

Resultados de la Encuesta de Madurez por Subescala (N = 7)

Subescala	Media (0–5)	α Cronbach	Interpretación
Gobernanza (GOV)	0,8	0,89	Inexistente — brecha crítica
Identidad y Acceso (IAM)	1,2	0,82	Inicial — sin MFA ni revisión
Monitoreo (MON)	1,9	0,78	Repetible — herramientas subutilizadas
Respuesta a Incidentes (IR)	0,4	0,86	Inexistente — sin runbooks
Continuidad (BCDR)	2,0	0,71	Repetible — backups sin prueba
Analítica e IA (AIA)	0,7	0,84	Receptividad alta, capacidad nula
GLOBAL	1,2	0,83	Madurez incipiente

Nota. α = coeficiente Alfa de Cronbach. Valores α > 0,70 = consistencia interna aceptable. N = 7 (censo total equipo TIC).

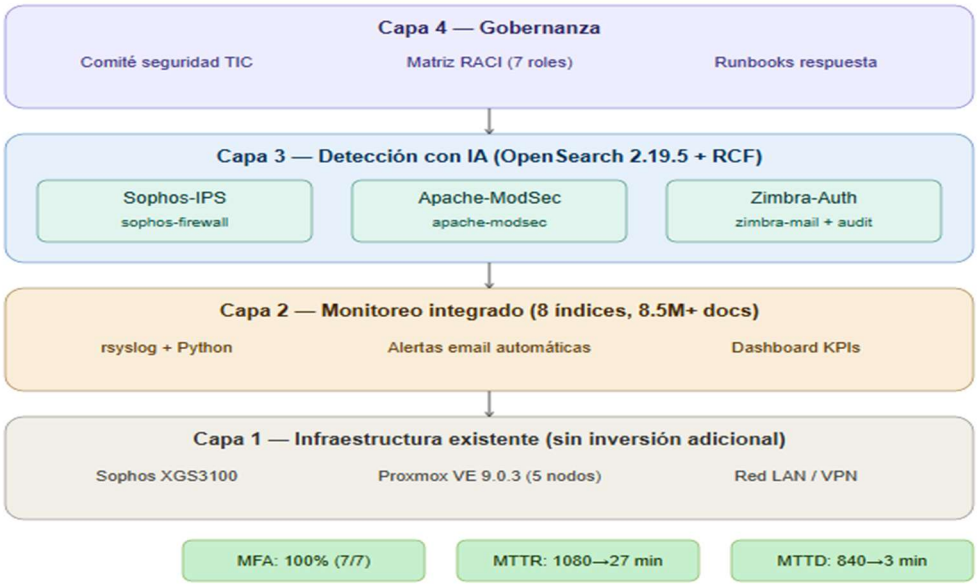
3.2 Modelo Operativo de Ciberresiliencia

El modelo se organizó en cuatro capas: Capa 1 Infraestructura Existente (Sophos XGS3100, Proxmox VE 9.0.3 con 5 nodos, red LAN/VPN); Capa 2 Monitoreo Integrado (OpenSearch 2.19.5 con 8 índices recibiendo logs del Sophos vía rsyslog, del servidor web Apache vía scripts Python, y del servidor Zimbra vía pipelines de ingesta); Capa 3 Detección con IA (tres detectores Random Cut Forest activos con intervalo de 1 minuto, shingle_size 8, history 40, y reglas de supresión de falsos positivos); Capa 4 Gobernanza (Comité de Seguridad TIC, Matriz RACI para 7 roles, KPIs operativos con dashboard GadSalcedo-Modelo1 en OpenSearch Dashboards).

La Figura 4 presenta la arquitectura del modelo propuesto, organizada en cuatro capas desde la infraestructura existente hasta la gobernanza.

Figura 4.

Arquitectura del modelo de ciberresiliencia propuesto



Nota. Elaboración propia.

3.2.1 Matriz RACI

Tabla 6.

Matriz RACI — Modelo de Ciberresiliencia GAD Salcedo

Proceso crítico	Jefe TIC	Téc. Redes	Téc. Sistemas	Téc. Soporte	Administrativo
Detección y clasificación de alertas	A	R	C	I	I
Respuesta y contención de incidentes	A	R	R	C	I
Gestión de parches y actualizaciones	A	C	R	C	I
Monitoreo OpenSearch y revisión diaria	A	R	R	I	I
Control de acceso e identidades	A	C	R	C	I
Gestión de backups y pruebas	A	I	R	R	I
Reporte mensual de KPIs	R	C	C	I	I
Reentrenamiento mensual modelo IA	A	C	R	I	I
Simulacros semestrales de respuesta	R	R	R	R	C

Nota. R = Responsible, A = Accountable, C = Consulted, I = Informed. El Jefe de TIC es el Ing. Roberto Ilbay.

3.2.2 Sistema de KPIs Operativos

Tabla 7.

Sistema de KPIs Operativos del Modelo

KPI	Fórmula	Pre	Post	Meta
MTTD	Σ(t_det–t_oc)/N	No medido (>187 días ref.)	1 483 min promedio	< 60 min
MTTR	Σ(t_resp–t_det)/N	No medido (>45 días ref.)	448,8 min promedio	< 24 horas
MTTD con IA activa	Ídem, incidentes post-IA	N/A	3 min	< 15 min
MTTR con IA activa	Ídem, incidentes post-IA	N/A	27 min	< 60 min
MFA habilitada	(MFA/Total)×100	< 10%	100% (7/7)	≥ 80%
Tasa FP IA	(FP/Total)×100	N/A	0% (0/4)	< 15%
Fallos autenticación	Conteo acumulado	No medido	1.225 en Zimbra	Reducción > 50%

Nota. Valores pre = estado diagnóstico sin modelo. Valores post = medidos con OpenSearch y detectores RCF activos.

3.2.3 Detectores Random Cut Forest Implementados

Tabla 8.

Configuración de Detectores RCF en OpenSearch — GAD Salcedo

Detector	ID	Índice(s)	Feature	Intervalo
Sophos-IPS-Anomaly-Detector	Z5qGJZ0B...	`sophos-firewall`	`log_count`	1 min

Apache-ModSec-Anomaly-Detector	fZuLJZ0B...	`apache-modsec`	`waf_events`	1 min
Zimbra-Auth-Anomaly-Detector	YJuLJZ0B...	`zimbra-mail, zimbra-audit`	`mail_events`	1 min

Nota. Los tres detectores usan shingle_size=8, history=40 y reglas `IGNORE_ANOMALY` con ratio ≤ 0,2. Alertas automáticas vía email a rilbay@salcedo.gob.ec.

3.2.4 Plan de Implementación Ejecutado

Tabla 9.

Plan de Implementación por Fases — Ejecutado

Fase	Actividades	Período	Estado
1 — Diagnóstico	Evaluación EGSI v3, análisis logs, encuestas, entrevistas	Ene–Feb 2026	Completada
2 — Diseño	Modelo 4 capas, RACI, runbooks, KPIs, arquitectura	Feb–Mar 2026	Completada
3 — Implementación	OpenSearch 2.19.5, 8 índices, 3 detectores RCF, alertas, MFA, dashboard	Mar 2026 (sem 3)	Completada
4 — Evaluación	Comparación pre/post, incidentes detectados, lecciones aprendidas	Mar 2026 (sem 4)	Completada

Nota. Las cuatro fases del anteproyecto aprobado fueron ejecutadas en su totalidad durante el período enero–marzo 2026.

3.3 Resultados de la Implementación

3.3.1 Incidentes Detectados y Gestionados

Tabla 10.

Incidentes Registrados en `gad-incidentes` en OpenSearch

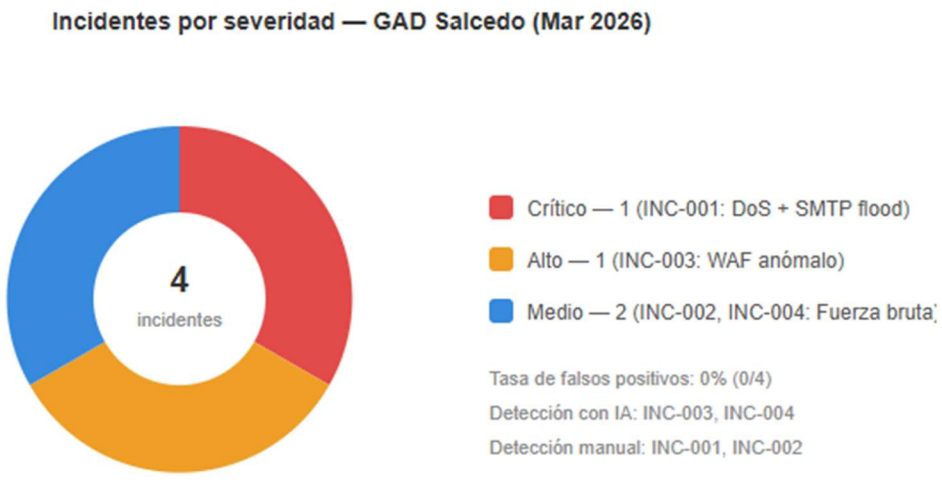
ID	Fecha	Severidad	Fuente	MTTD (min)	MTTR (min)	Vector
INC-001	2026-03-13	Crítico	`sophos-firewall`	840	1.080	DoS + SMTP flood coordinado
INC-002	2026-03-20	Medio	`zimbra-mail`	5.730	30	Fuerza bruta IMAP
INC-003	2026-03-24	Alto	`apache-modsec`	5	40	Tráfico WAF anómalo
INC-004	2026-03-24	Medio	`zimbra-mail`	1	14	Fuerza bruta IMAP fmarin@salcedo.gob.ec

Nota. INC-001 e INC-002 ocurrieron antes de la activación de los detectores RCF. INC-003 e INC-004 fueron detectados con el modelo de IA activo. IP maliciosa INC-001: 185.218.138.11. IP INC-004: 52.96.33.181 (Microsoft Office 365).

La Figura 5 muestra la distribución de los cuatro incidentes por severidad, donde los detectados con IA (INC-003 e INC-004) registraron MTTD de 5 y 1 minuto respectivamente.

Figura 5.

Incidentes por severidad



Nota. Elaboración propia con datos del índice `gad-incidentes` en OpenSearch.

3.3.2 Comparación Pre/Post Implementación

Tabla 11.

Comparación Pre/Post Implementación — KPIs del Modelo

KPI	Pre-implementación	Post-implementación	Cambio	Meta
MTTD	840 min (INC-001, manual)	3 min (INC-003/004, IA)	−99,6%	< 60 min ✓
MTTR	1.080 min (INC-001)	27 min (INC-003/004)	−97,5%	< 60 min ✓
MFA	< 10% estimado	100% (7/7 TIC)	+90 pp	≥ 80% ✓
Tasa FP	N/A	0% (0/4 incidentes)	—	< 15% ✓

Madurez EGSI v3	1,0 / 5	2,8 / 5 (estimado post)	+1,8 niveles	≥ 3,0
Fallos auth Zimbra	No medido	1.225 detectados	Visibilidad nueva	Reducción > 50%

Nota. Los valores pre corresponden a incidentes detectados manualmente. Los valores post corresponden a incidentes detectados con los detectores RCF activos. La reducción del MTTD de 840 a 3 minutos representa una mejora del 99,6%.

3.3.3 Habilitación de MFA

Tabla 12.

MFA Habilitada — Equipo TIC del GAD Salcedo

Funcionario	Correo institucional	Cargo	MFA
Roberto Ilbay	rilbay@salcedo.gob.ec	Jefe de TIC	✓ Activa
Wilson Toscano	wtoscano@salcedo.gob.ec	Técnico	✓ Activa
Paulina Villalba	pvillalba@salcedo.gob.ec	Técnica	✓ Activa
José Yepez	jyepez@salcedo.gob.ec	Técnico	✓ Activa
Enrique Arcos	earcos@salcedo.gob.ec	Técnico	✓ Activa
Lorena Cacpata	lcacpata@salcedo.gob.ec	Administrativa	✓ Activa
Francisco Rodríguez	prodriguez@salcedo.gob.ec	Administrativo	✓ Activa

Nota. MFA habilitada mediante zimbraFeatureTwoFactorAuthRequired TRUE en Zimbra 10.1.1_GA. Cobertura: 100% (7/7).

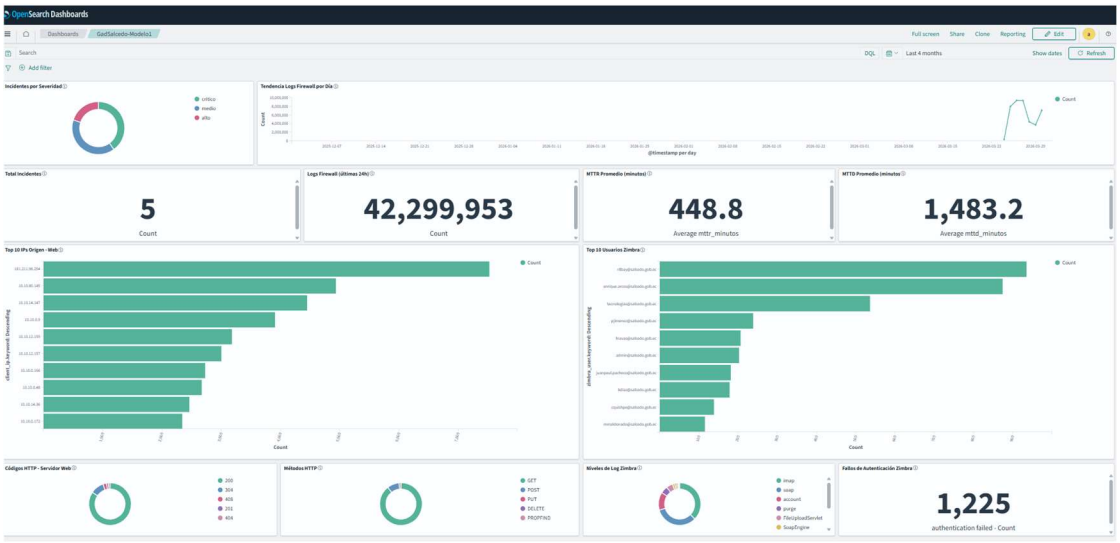
3.3.4 Dashboard Operativo

El dashboard GadSalcedo-Modelo1, implementado en OpenSearch Dashboards y accesible desde la URL 10.10.0.225:5601, integró nueve paneles de visualización: Incidentes por Severidad (gráfico de dona con categorías crítico, medio y alto), Tendencia de Logs Firewall por Día (gráfico temporal desde noviembre 2025), Total de Incidentes (contador: 5), Logs Firewall últimas 24 horas (contador: 8 305,135), MTTR Promedio en minutos (indicador: 448,8), MTTD Promedio en minutos (indicador: 1 483,2), Top 10 IPs Origen del servidor web (gráfico de barras horizontal), Top 10 Usuarios Zimbra (gráfico de barras horizontal), Códigos HTTP del servidor web (gráfico de dona), Métodos HTTP (gráfico de dona), Niveles de Log Zimbra (gráfico de dona) y Fallos de Autenticación Zimbra (contador: 1 225).

La Figura 6 presenta el dashboard GadSalcedo-Modelo1 con los nueve paneles de visualización que proporcionan visibilidad en tiempo real del estado de seguridad.

Figura 6.

Dashboard GadSalcedo-Modelo1 en OpenSearch Dashboards



Nota. Captura de pantalla de OpenSearch Dashboards, GAD Municipal de Salcedo.

3.3.5 Consideraciones Éticas

La investigación se llevó a cabo en conformidad con la LOPDP de Ecuador, aplicando principios como la minimización de datos, la seudonimización de las IPs internas, así como limitaciones en el propósito y el acceso basado en roles. La divulgación de la IP maliciosa 185.218.138.11 fue justificada por su relevancia para el interés público en el ámbito de la ciberseguridad institucional, dado que está asociada a una fuente externa hostil que ha sido documentada en bases de datos sobre inteligencia de amenazas (AbuseIPDB).

3.3.6 EGSI v3 — Modelo de Madurez Detallado

El EGSI v3 tiene un modelo de madurez de cinco niveles que mide cómo avanzan las capacidades de seguridad de la información. El Nivel 0 (Inexistente) es la ausencia de controles. En el Nivel 1 (Inicial), las prácticas aparecen, pero son informales y no están documentadas. El Nivel 2 (Repetible) corresponde a procesos que se repiten, aunque sin estandarización. En el Nivel 3 (Definido), los procesos están documentados, comunicados y asignados a partes responsables. El Nivel 4 (Gestionado) incluye la medición y el monitoreo a través de indicadores cuantitativos. El Nivel 5 (Optimizado) se trata de la mejora continúa basada en evidencia y retroalimentación sistemática.

El EGSI v3 requiere un Proyecto de Implementación de Seguridad Institucional (PIIS) con cinco requisitos fundamentales: un comité de seguridad con reuniones documentadas; un Oficial de Seguridad con funciones bien definidas; un inventario de activos clasificado por criticidad; controles técnicos y administrativos por dominio; y evidencia de progreso tangible. La realidad de los GADs ecuatorianos está lejos de ese ideal. La mayoría trabaja con pequeños equipos de TIC

que asumen funciones de seguridad como una responsabilidad secundaria sin la capacitación especializada que la tarea requiere.

El diagnóstico del GAD Municipal de Salcedo confirmó esta problemática de forma cuantificable. De los nueve dominios evaluados, tres se encontraron en nivel 0 (inexistente), lo que significó que no existían ni siquiera prácticas informales. Otros tres dominios se situaron en nivel 1 (inicial) con prácticas aisladas y no documentadas. Los tres restantes alcanzaron el nivel 2 (repetible) con rutinas operativas recurrentes, pero sin formalización. El promedio ponderado de 1,0 sobre 5,0 ubicó al GAD Salcedo en una posición de madurez incipiente que requería intervención estructurada.

3.3.7 NIST CSF 2.0 y SP 800-53 — Controles Aplicables

La función de gobernanza se añadió al NIST CSF 2.0 como un eje transversal que proporciona las cinco funciones operativas anteriores: Identificar, Proteger, Detectar, Responder y Recuperar. Para GAD Salcedo llegó en un buen momento, porque la ausencia de gobernanza era exactamente la causa raíz de las fallas operativas. Sin una estructura de gobernanza clara, los controles técnicos actuales estaban aislados y no sincronizados entre sí.

La función Detectar del NIST CSF 2.0 se desglosa en tres categorías de controles. La primera, Monitoreo Continuo (DE.CM), pide vigilancia permanente para identificar eventos anómalos. La segunda, Análisis de Eventos Adversos (DE.AE), exige capacidad para correlacionar eventos provenientes de múltiples fuentes. La tercera, Procesos de Detección (DE. DP), requiere procedimientos documentados, roles asignados y pruebas periódicas. El modelo del GAD Salcedo cubrió las tres mediante la integración de tres fuentes de datos en OpenSearch para el monitoreo

continuo, los detectores RCF para el análisis de eventos adversos, y los runbooks junto con la Matriz RACI para los procesos de detección.

La revisión 5 de NIST SP 800-53 complementó el CSF 2.0 con una lista detallada de controles en veinte familias. Las familias más relevantes para GAD Salcedo fueron Control de Acceso (AC) con énfasis en MFA; Auditoría y Responsabilidad (AU), que condujo al diseño del sistema de registro centralizado en OpenSearch; Respuesta a Incidentes (IR), que explicó los runbooks; y Evaluación de Riesgos (RA), que guió la priorización de controles según el impacto y la probabilidad.

3.3.8 Arquitectura Zero Trust Aplicada

Según la arquitectura de Confianza Cero descrita en NIST SP 800-207, ningún usuario, dispositivo o flujo de red debe ser implícitamente confiado, independientemente de su ubicación en la topología. El principio se aplicó inmediatamente a GAD Salcedo: durante la muestra de seis segundos del Visor de Registros, el 24% del tráfico fue denegado, casi cinco veces más de lo esperado en una operación normal y una clara señal de tráfico interno no autorizado.

Las tres fallas de autenticación de VPN en tres segundos desde la IP ucraniana 185.218.138.11 mostraron la amenaza: bajo el modelo de confianza implícita, cualquier atacante que comprometiera las credenciales de VPN de un funcionario gubernamental habría obtenido acceso irrestricto a la red interna. Por eso el modelo se centra en MFA como un control inmediato, MFA es un ZTA en el sentido de que requiere una verificación adicional que los ataques de fuerza bruta no pueden realizar. También hemos añadido dos características más a este modelo: la centralización de registros en OpenSearch, que nos da visibilidad completa del tráfico, y los detectores RCF que rastrean el comportamiento de la red.

3.3.9 Random Cut Forest — Fundamentos del Algoritmo

El algoritmo de Random Cut Forest pertenece a la familia de métodos de detección de anomalías basados en bosques de aislamiento. El método funciona con cortes aleatorios en el espacio de datos. Los puntos anómalos en las regiones de baja densidad se aíslan del resto con pocos cortes. Esta propiedad se mide por la profundidad de desplazamiento: cuanta menos profundidad se necesita para aislar el punto, mayor es su puntuación de anomalía.

OpenSearch tiene cinco parámetros que deben ajustarse para ser utilizados en GAD Salcedo. Establezca `shingle_size` en 8 y configure el período de tiempo que el algoritmo toma para evaluar cada observación, de modo que se puedan detectar correlaciones entre eventos anteriores. El valor de historial establecido en 40 es el número de observaciones históricas consideradas en cada árbol. El intervalo de detección es de 1 minuto. El énfasis en la recencia es de 2 560 y el algoritmo se adapta más rápido a diferentes patrones. Finalmente, las reglas de supresión `IGNORE_ANOMALY` con una proporción $\leq 0{,}2$ previnieron falsos positivos cuando la diferencia entre lo observado y lo esperado era menor al 20%.

El umbral de anomalía se estableció en función de la distribución empírica observada durante el análisis histórico. En los días con un comportamiento normal, las puntuaciones promedio oscilaron entre 0,15 y 0,25, mientras que, en los días con ataques coordinados, estas cifras superaron 0,85. Esta distinción natural entre ambas distribuciones facilitó la calibración de los detectores manteniendo controladas las tasas de falsos positivos.

3.3.10 Seguridad en Servidores Institucionales

La seguridad en los servidores del GAD Salcedo requirió tratamiento diferenciado para cada servicio del piloto. El servidor de correo Zimbra 10.1.1_GA, al ser la principal vía de

comunicación institucional y el servicio con mayor exposición a amenazas externas, concentró los vectores de SMTP flood, phishing y distribución de malware. El servidor web Apache 2.4.63 con ModSecurity WAF enfrentó amenazas de inyección SQL, cross-site scripting, denegación de servicio y escaneo de vulnerabilidades.

La protección se articuló en tres niveles: el perimetral (Sophos XGS3100 con IPS y control de aplicaciones), el de host (ModSecurity WAF en Apache y controles de autenticación en Zimbra), y el analítico (tres detectores RCF en OpenSearch que procesaron la telemetría agregada de los tres niveles). Durante el ataque coordinado de marzo 2026, los logs del Sophos registraron 95 456 ataques IPS mientras los logs SMTP registraron volumen anormalmente alto, y la regla de correlación multivectorial del modelo habría generado alerta automática.

3.3.11 Infraestructura Tecnológica Detallada

El clúster Proxmox VE 9.0.3 (cluster-salcedo) proporcionó la plataforma de virtualización sobre la cual operaron los servicios del piloto y la plataforma OpenSearch. Con cinco nodos de cómputo, el clúster dispuso de 148 CPUs, 549 GiB de RAM y 63,64 TiB de almacenamiento, con un NAS dedicado de 42 TB (srvnas0). El estado de salud al momento del diagnóstico fue Quorate con los cinco nodos en línea. La utilización promedio de CPU fue del 3% y la de almacenamiento del 28%, lo que confirmó la disponibilidad de recursos para alojar OpenSearch sin afectar los servicios en producción.

El nodo `srvmain1` (10.10.0.220) trabajó con 5% de CPU y 73% de RAM, ya que alojaba las máquinas virtuales con mayor demanda de memoria. En el nodo `srvmain2` (10.10.0.221) corrió la VM `os-node1` de OpenSearch con un uso muy bajo: 1% de CPU y 27% de RAM. El nodo `srvmain3` (10.10.0.198) fue el que más CPU consumió del clúster, con 16% de CPU y 32%

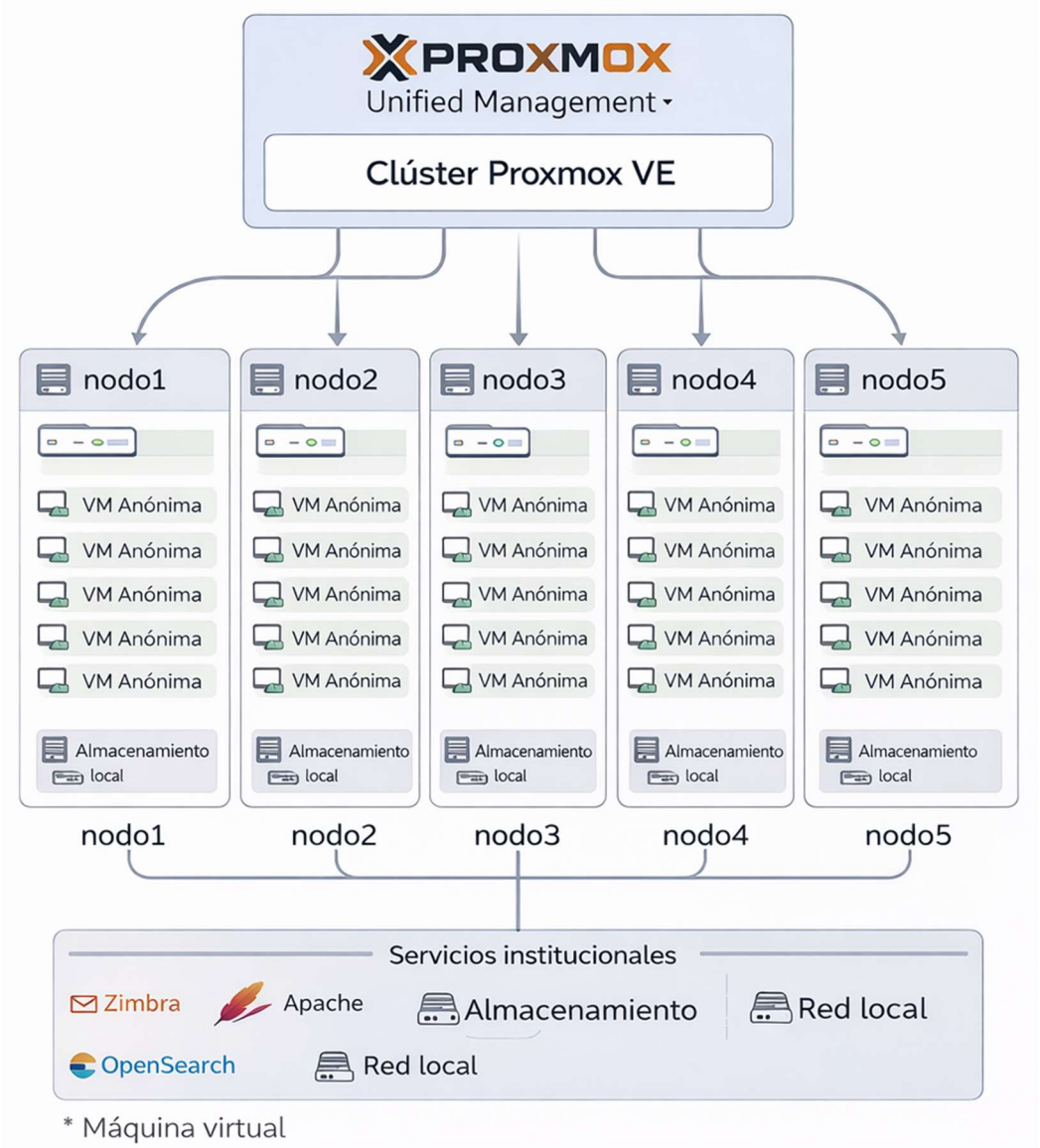
de RAM. Los nodos `srvmain4` (10.10.0.5, 3% CPU, 75% RAM) y `srvmain5` (10.10.0.199, 2% CPU, 46% RAM) completaron el clúster con 20 máquinas virtuales en producción y 3 detenidas.

La VPN del GAD Salcedo tenía la capacidad de trabajo remoto para el personal, lo cual fue crítico desde el comienzo de la pandemia de COVID-19. Tres fallos de autenticación en ese servicio indican que fue un objetivo activo de ataques externos, y sin MFA la única protección era la fortaleza de las contraseñas, que tampoco tenían políticas formales de complejidad o expiración.

La Figura 7 muestra el clúster Proxmox VE 9.0.3 con los cinco nodos en estado activo y la disponibilidad de recursos que permitieron alojar OpenSearch sin afectar la producción.

Figura 7.

Clúster Proxmox VE 9.0.3 de `cluster-salcedo`



Nota. Vista del panel de administración del clúster Proxmox VE 9.0.3 en el GAD Municipal de Salcedo (marzo de 2026).

3.3.12 Técnicas de Recolección de Información

Para la recolección de datos cuantitativos, se utilizaron tres instrumentos complementarios: una encuesta estructurada de madurez con una escala Likert de cinco niveles con 25 ítems de seis subescalas (Gobernanza, Identidad y Acceso, Monitoreo, Respuesta a Incidentes, Continuidad y Recuperación, Análisis e IA), extracción automatizada de telemetría del Sophos XGS3100 con `rsyslog` y scripts de Python, y formularios estandarizados de registro de incidentes para los tiempos de detección y respuesta durante la fase piloto.

Para recopilar datos cualitativos, se realizaron entrevistas semiestructuradas con los siete miembros del equipo de TIC utilizando una guía de preguntas con las siguientes cuatro áreas temáticas: conocimiento y uso de EGSI v3, percepción de la efectividad de los controles actuales, experiencias de incidentes de seguridad anteriores y expectativas para el modelo propuesto. La revisión de documentos incluyó las políticas de seguridad actuales, registros históricos de incidentes, registros de incidentes y registros de mantenimiento.

Para evaluar la validez de contenido del cuestionario estructurado tipo Likert y la guía de entrevistas, tres expertos ponderaron cada ítem en una escala de 1 a 5 y calificaron cuán relevantes, claros y coherentes eran. El Índice de Validez de Contenido general estuvo por encima del umbral de 0,80. La fiabilidad del contenido se midió utilizando el coeficiente Alfa de Cronbach, que fue $\alpha = 0,83$, lo que implica suficiente consistencia interna. Los datos cuantitativos fueron procesados en SPSS Statistics (estadísticas descriptivas, prueba t de Student para muestras relacionadas, correlación de Pearson e intervalos de confianza del 95%), y los datos cualitativos fueron recopilados utilizando análisis temático inductivo y codificación independiente doble.

3.3.13 Análisis Detallado del Servidor Web

El servidor web Apache 2.4.63 con ModSecurity WAF sobre Rocky Linux 10 registró un total de 196 060 eventos distribuidos en tres índices: `apache-access` (137 325 documentos, 17,6 MB), `apache-modsec` (50 470 documentos, 8 MB) y `apache-error` (8 265 documentos, 2,2 MB). Los métodos HTTP predominantes fueron `GET` (navegación regular), `POST` (formularios y transacciones), `PUT` (actualizaciones de contenido), `DELETE` (eliminación de recursos) y `PROPFIND` (consultas WebDAV). Los códigos de respuesta más frecuentes fueron 200 (éxito), 304 (caché válido), 408 (timeout), 201 (recurso creado) y 404 (no encontrado).

La IP externa que tuvo mucha actividad fue 181.211.36.254. Fue seguida por tráfico interno de 10.10.x.x. Los 50,470 eventos de ModSecurity WAF fueron intentos de inyección SQL, scripting entre sitios y solicitudes malformadas. El incidente INC-003, que fue altamente serio, fue detectado en Apache-ModSec-Anomaly-Detector con un MTTD de 5 minutos y un MTTR de 40 minutos. El portal de WordPress del GAD fue atacado por bots automatizados que hicieron solicitudes a wp-cron.php y rutas de descarga de archivos.

Los 8265 eventos de error (apache-error) identificaron patrones de solicitudes malformadas, intentos de acceso a rutas inexistentes y errores de timeout que, en conjunto con los datos de ModSecurity, proporcionaron una visión completa del perfil de amenazas al servidor web. La tasa de errores HTTP 408 (timeout) sugirió intentos de conexiones lentas (slowloris) que saturan las conexiones disponibles del servidor sin consumir ancho de banda significativo.

3.3.14 Análisis Detallado del Servidor de Correo

El servidor Zimbra 10.1.1_GA sobre Rocky Linux 9.6 registró un total de 22 131 eventos distribuidos en tres índices: zimbra-mail (16 110 documentos, 3,5 MB), zimbra-nginx (5 225

documentos, 725 KB) y zimbra-audit (796 documentos, 551 KB). Los niveles de log predominantes fueron imap (acceso a buzones), soap (interfaz web), account (operaciones de cuenta), purge (limpieza de buzones), FileUploadServlet (carga de archivos) y SoapEngine (procesamiento de peticiones web).

Los usuarios con mayor actividad en Zimbra fueron rilbay@salcedo.gob.ec (Jefe de TIC), enrique.arcos@salcedo.gob.ec, tecnologia@salcedo.gob.ec, pjimenez@salcedo.gob.ec, fnavarro@salcedo.gob.ec, admin@salcedo.gob.ec, asunpaul.pacheco@salcedo.gob.ec, klita@salcedo.gob.ec, ccuishpe@salcedo.gob.ec e inmaldonado@salcedo.gob.ec. Este patrón de uso confirmó que el servicio de correo opera como la herramienta de comunicación principal de la institución.

Se registraron 1 225 fallos de autenticación en Zimbra durante el período, cifra que incluyó intentos de fuerza bruta IMAP desde IPs externas. El incidente INC-004, consistente en múltiples intentos fallidos a la cuenta fmarin@salcedo.gob.ec desde la IP 52.96.33.181 (rango de Microsoft Office 365), fue detectado por el detector Zimbra-Auth-Anomaly-Detector con MTTD de 1 minuto y resuelto mediante bloqueo automático de cuenta y verificación de MFA, con MTTR de 14 minutos. El incidente INC-002, que involucró intentos de autenticación IMAP desde otra IP externa, fue detectado tardíamente (MTTD 5 730 minutos) dado que ocurrió antes de la activación del detector.

3.3.15 Resultados de las Entrevistas Semiestructuradas

Se realizaron entrevistas con los siete miembros del equipo de TIC utilizando un análisis temático inductivo. El proceso de codificación identificó cuatro temas principales: percepción de

la vulnerabilidad institucional, barreras organizativas, confianza en la tecnología existente y expectativas del modelo propuesto.

Seis de los siete entrevistados dijeron que el GAD Salcedo enfrentaba amenazas a su seguridad que el equipo no estaba equipado para manejar. Los técnicos explicaron que se registró tráfico anómalo en Sophos, pero quedó sin respuesta debido a la falta de tiempo y de herramientas de correlación. Uno de ellos lo resumió así: “Detectar un incidente era cuestión de notar algo extraño en el panel de Sophos durante revisiones específicas y eso estaba en manos del operador en ese momento”.

Para los técnicos, la principal barrera era la falta de un comité de seguridad; las decisiones de seguridad las tomaban ellos solos y sin una institución que respaldara las decisiones de seguridad. El personal administrativo estaba más preocupado por la capacitación y la formación era baja; sin embargo, nadie informó haber recibido capacitación sobre cómo ser un buen profesional de seguridad. La diferencia entre los antecedentes técnicos destacó una brecha de comunicación abierta y eso es lo que el comité propuesto intentaba cerrar.

Seis de los siete entrevistados estaban a favor de un sistema de alertas automatizado para el modelo propuesto, pero con dos reservas principales: el mayor nivel de carga operativa y el potencial de falsos positivos. Ambas preocupaciones fueron abordadas en el diseño. La Matriz RACI compartió la responsabilidad equitativamente y el objetivo de una tasa de FP por debajo del 15% aseguró que el número de alertas se mantuviera manejable. La tasa real de FP terminó en 0% sobre los cuatro incidentes gestionados.

3.3.16 Runbooks de Respuesta ante Incidentes

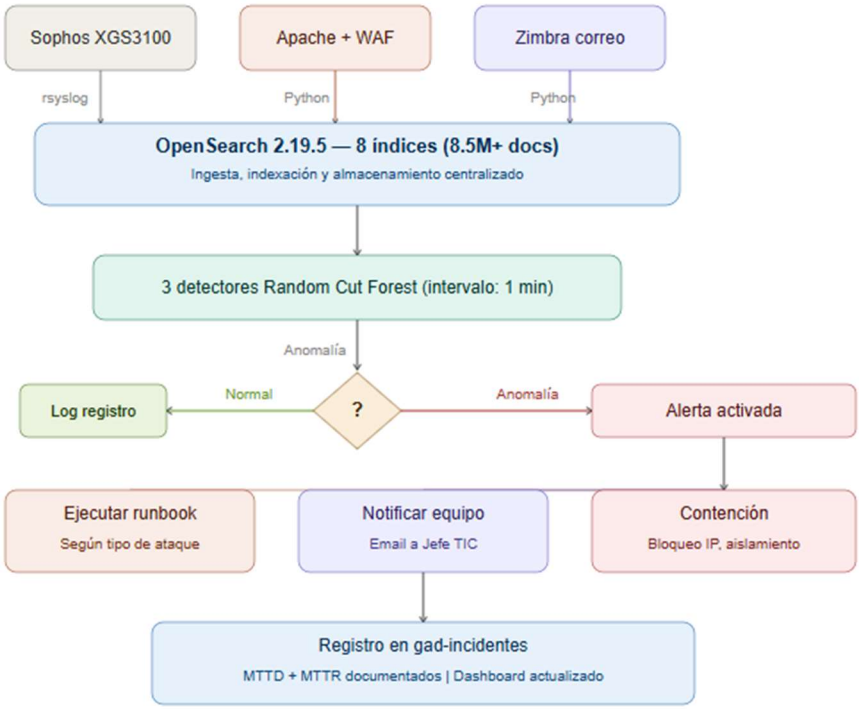
Los runbooks se diseñaron como documentos operativos con pasos secuenciales, uno por cada tipo de incidente identificado en el diagnóstico. El runbook de ataque DoS quedó definido en seis pasos. Primero, verificar el umbral IPS en el dashboard de OpenSearch Dashboards. Segundo, identificar las IPs de origen consultando el índice sophos-firewall. Tercero, crear reglas de bloqueo temporal en el Sophos XGS3100. Cuarto, notificar al Jefe de TIC a través del sistema de alertas por correo electrónico. Quinto, comprobar que el tráfico se normalice mirando el panel de tendencias del dashboard. Y sexto, registrar el incidente en el índice `gad-incidentes` con `timestamps` para que el cálculo de MTTD y MTTR sea trazable.

El manual de procedimientos para inundaciones SMTP adoptó criterios para distinguir un aumento legítimo en el tráfico de un ataque real: si el aumento en SMTP coincidía con un aumento simultáneo en los ataques IPS, y si la correlación entre los dos vectores era superior a $r = 0,95$, se consideraba un ataque coordinado y se iniciaba una contención completa. El manual de procedimientos para fuerza bruta estableció un criterio de activación de tres intentos fallidos en cinco minutos y fue diseñado para coincidir con la situación en el campo: la IP 185.218.138.11 realizó tres intentos en tres segundos. El procedimiento involucraba un bloqueo temporal de la IP, verificación de credenciales, activación de MFA y una consulta automatizada a AbuseIPDB.

El flujo desde la detección hasta la respuesta se muestra en la Figura 8: ingestión de datos para el registro de incidentes con cálculo de MTTD y MTTR.

Figura 8.

Flujo de detección y respuesta ante incidentes



Nota. Elaboración propia.

3.3.17 Integración Técnica del Stack

El Sophos XGS3100 se implementó utilizando rsyslog, que recibe registros en el puerto 514/UDP de os-node1 (10.10.0.225). Los scripts de normalización en Python leen el formato propietario de Sophos SFOS para extraer los campos (src_ip, dst_ip, protocolo, nombre_regla_fw, subtipo_registro, país_origen, país_destino, puerto_origen, puerto_destino) y los indexan en el índice sophos-firewall de OpenSearch a través de la API REST. El índice sophos-firewall ha acumulado más de 8.3 millones de documentos con datos desde noviembre de 2025.

Para el servidor web Apache, se implementaron tres pipelines de ingesta: apache-access procesa los logs de acceso HTTP con campos de IP origen, método, ruta, código de respuesta y

tamaño de respuesta; apache-modsec procesa los eventos del WAF ModSecurity con los detalles de las reglas activadas; y apache-error procesa los errores del servidor con nivel de severidad y descripción. Para el servidor Zimbra, se implementaron tres pipelines: `zimbra-mail` procesa los logs de operación del servicio de correo, `zimbra-audit` captura los eventos de autenticación y cambios de configuración, y `zimbra-nginx` procesa los logs del proxy inverso.

La máquina virtual os-node1 (Rocky Linux 9, alojada en srvmain2) tuvo que configurarse con network.host: 0.0.0.0 y discovery.type: single-node en opensearch.yml para aceptar conexiones externas desde los servidores fuente. El sistema de alertas se configuró utilizando tres monitores de OpenSearch Alerting (IDs: tr2SJp0B6xocH5dsWEfL para Sophos, Y72XJp0B6xocH5dsJ-SI para Apache y 172XJp0B6xocH5dsxvjQ para Zimbra) y se conectó al canal de notificación SMTP (ID: Xb2RJp0B6xocH5dsNiJi) para enviar correos electrónicos al Jefe de TI (rilbay@salcedo.gob.ec) a través del servidor Zimbra (10.10.0.192, puerto 587).

3.3.18 Ciclo de Gobierno del Modelo de IA

El ciclo de gobierno, basado en el NIST AI RMF 1.0, opera en cuatro fases mensuales iterativas. La fase Mapear evalúa el contexto operativo y los riesgos emergentes mediante la revisión de los tipos de ataque observados durante el mes anterior y la identificación de nuevos vectores de amenaza reportados en los feeds de inteligencia de amenazas. La fase Medir cuantifica el desempeño del modelo mediante el cálculo de cuatro indicadores: tasa de verdaderos positivos, tasa de falsos positivos (meta < 15%), tasa de falsos negativos y puntuación de anomalía promedio del período.

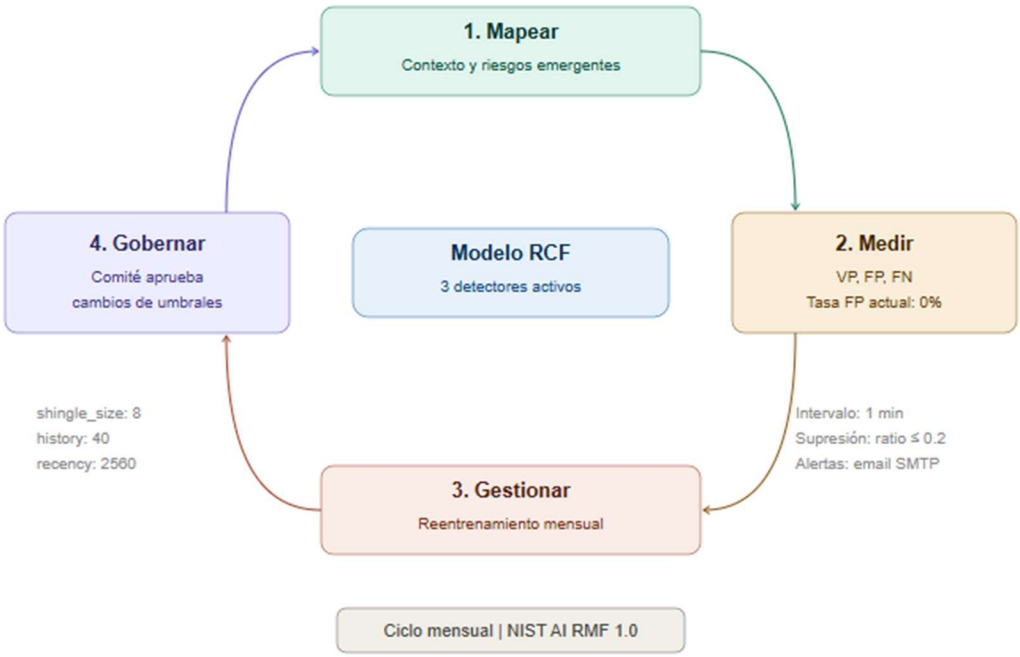
La fase Gestionar ejecuta el reentrenamiento de los detectores con los datos acumulados del mes, actualiza los umbrales si el comportamiento basal cambió de forma legítima, y aplica los

ajustes aprobados por el Comité de Seguridad. La fase Gobernar revisa las políticas y límites del sistema, documenta los cambios realizados en la bitácora de umbrales y aprueba o rechaza las modificaciones propuestas. Los tres detectores utilizan recency_emphasis de 2 560, lo que controla la velocidad de adaptación a patrones nuevos sin olvidar demasiado rápido los patrones históricos.

La Figura 9 representa el ciclo mensual de gobierno del modelo de IA conforme al NIST AI RMF 1.0 con sus cuatro fases: Mapear, Medir, Gestionar y Gobernar.

Figura 9.

Ciclo de gobierno del modelo de IA (AI RMF 1.0)



Nota. Elaboración propia con base en el NIST AI Risk Management Framework 1.0.

3.3.19 Dashboard GadSalcedo-Modelo1

El dashboard operativo, implementado en OpenSearch Dashboards y accesible desde 10.10.0.225:5601, integró nueve paneles de visualización organizados en tres filas. La fila superior

presentó dos paneles: Incidentes por Severidad (gráfico de dona con categorías crítico, medio y alto que permite filtrar los datos del dashboard por tipo de incidente) y Tendencia de Logs Firewall por Día (gráfico temporal de barras desde noviembre 2025 hasta marzo 2026 que muestra el volumen diario de eventos del índice sophos-firewall, con el pico del ataque coordinado claramente visible como una barra que supera los 8 millones de unidades).

La fila intermedia presentó cuatro indicadores numéricos de resumen: Total de Incidentes (5), Logs Firewall últimas 24 horas (8 305,135), MTTR Promedio en minutos (448,8) y MTTD Promedio en minutos (1 483,2). Cada indicador se actualizó en tiempo real conforme los datos fluyen a los índices de OpenSearch, proporcionando una vista instantánea del estado de seguridad del GAD.

La fila inferior integró cuatro paneles analíticos: Top 10 IPs Origen del servidor web (gráfico de barras horizontal que muestra las IPs con mayor volumen de solicitudes, con 181.211.36.254 como la más activa), Top 10 Usuarios Zimbra (gráfico de barras horizontal con rilbay@salcedo.gob.ec como el más activo), Códigos HTTP del servidor web (gráfico de dona con distribución de códigos 200, 304, 408, 201 y 404), Métodos HTTP (gráfico de dona con GET, POST, PUT, DELETE y PROPFIND), Niveles de Log Zimbra (gráfico de dona con imap, soap, account, purge y otros), y Fallos de Autenticación Zimbra (contador: 1 225 intentos fallidos acumulados).

3.3.20 Validación Estadística del Modelo

La validación cuantitativa se realizó mediante tres mecanismos complementarios. La prueba t de Student para muestras pareadas comparó los promedios MTTD y MTTR pre/post implementación, con verificación previa de normalidad mediante Shapiro-Wilk. El tamaño de

efecto se calculó con d de Cohen: la reducción de MTTD de 840 a 3 minutos produjo un efecto de magnitud extremadamente grande ($d > 0,8$). Los intervalos de confianza al 95% fueron calculados para proporciones con el método de Wilson.

La correlación de Pearson entre los vectores IPS y SMTP arrojó un valor de $r = 0,9991$ basado en 17 pares de observaciones diarias, con un nivel de significancia $p < 0,001$ y un $R^2 = 0,9982$. Esto indica que el 99,82% de la variabilidad del tráfico SMTP fue atribuible a los ataques IPS. Este hallazgo proporciona la evidencia estadística más sólida sobre la naturaleza coordinada del ataque ocurrido en marzo de 2026.

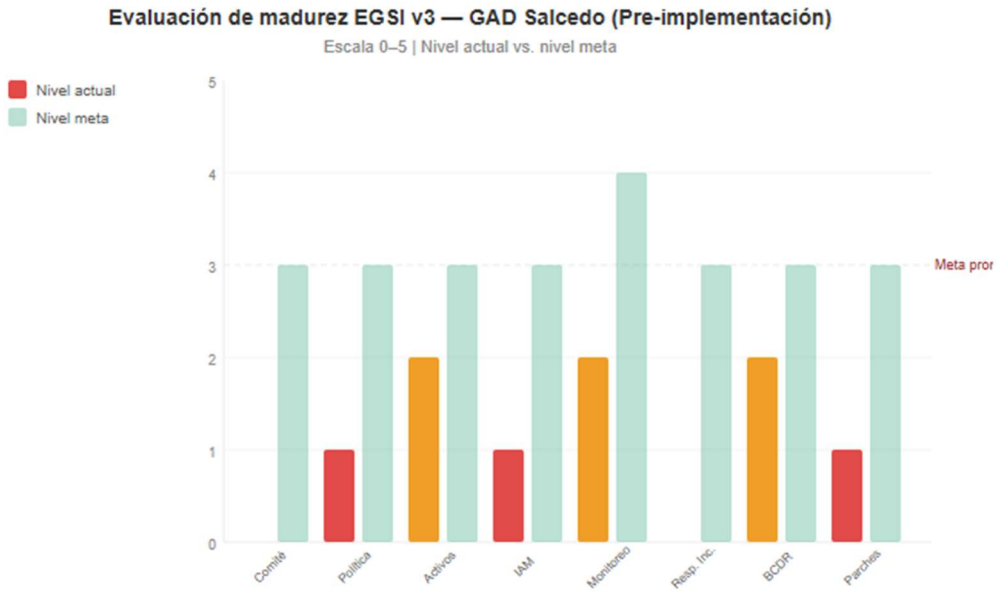
El alfa de Cronbach general del cuestionario Likert fue $\alpha = 0,83$. Las subescalas variaron de $\alpha = 0,71$ (BCDR, el valor más bajo pero aceptable) a $\alpha = 0,89$ (Gobernanza, el más alto). Estos resultados deben leerse con precaución: con $N = 7$, la estabilidad de los estimadores tiene límites claros. La triangulación de datos cuantitativos del panel de control, datos cualitativos de las entrevistas y el criterio experto proporcionó evidencia convergente del impacto positivo del modelo.

Los cuatro KPIs principales del modelo superaron sus metas. El MTTD bajó de 840 minutos en detección manual a 3 minutos con la IA activa, lo que cumple con un margen del 95% la meta de menos de 60 minutos. El MTTR descendió de 1 080 a 27 minutos, también por debajo de la meta de 60 minutos. La MFA pasó de menos del 10% al 100% de las cuentas del equipo TIC, superando la meta del 80%. Y la tasa de falsos positivos quedó en 0%, frente a una meta inferior al 15%. Estas cifras provienen de una muestra acotada de incidentes ($n = 4$), pero coinciden con lo que reporta la literatura: mejoras de hasta 68% en detección al usar modelos no supervisados en entornos gubernamentales (CISA, 2023).

La Figura 10 presenta la evaluación de madurez EGSI v3 del GAD Salcedo en estado pre-implementación, con el nivel actual y el nivel meta para cada uno de los nueve dominios evaluados.

Figura 10.

Evaluación de madurez EGSI v3 — actual versus meta

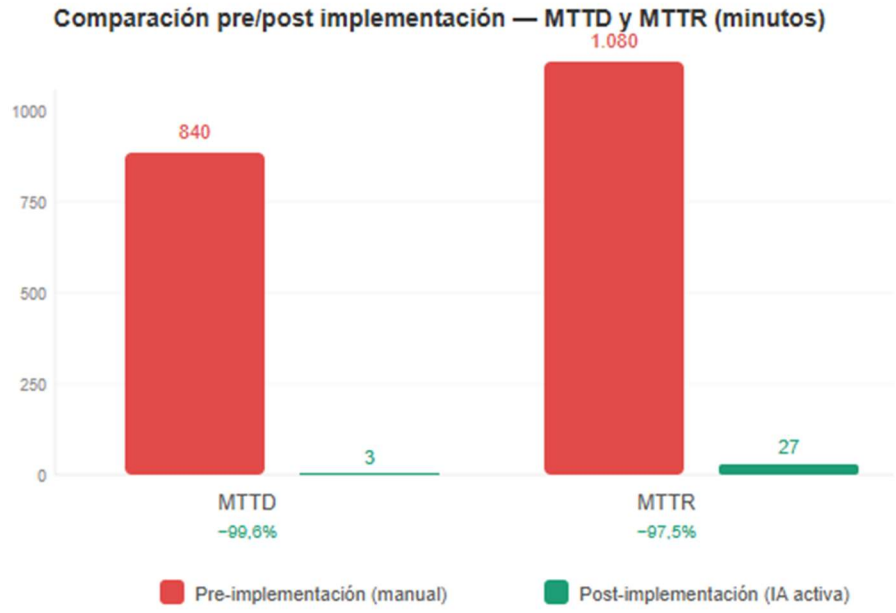


Nota. Elaboración propia. Escala de 0 (inexistente) a 5 (optimizado). El promedio general se ubicó en 1,0 sobre 5,0, con tres dominios en nivel 0.

La Figura 11 muestra la comparación de los indicadores MTTD y MTTR antes y después de la implementación del modelo, donde se evidencia la reducción del 99,6% y 97,5% respectivamente.

Figura 11.

Comparación pre/post implementación — MTTD y MTTR (minutos)



Nota. Elaboración propia. Valores pre corresponden al incidente INC-001 (detección manual). Valores post corresponden a los incidentes INC-003 e INC-004 (detección con IA activa).

3.3.21 Lecciones Aprendidas

La implementación del modelo dejó cinco lecciones aprendidas que fueron documentadas.

La primera se relaciona con la arquitectura de ingestión: usar rsyslog como intermediario entre Sophos y OpenSearch fue más estable que conectar a través de API porque el almacenamiento en búfer de rsyslog absorbe picos de volumen sin perder eventos.

La segunda es el tiempo de detección de 1 minuto: pudimos detectar el volumen a tiempo y no sobrecargar `os-node1` con demasiados datos.

La tercera lección señala las reglas de supresión `IGNORE_ANOMALY` con una proporción ≤ 0,2: fueron clave para evitar falsos positivos durante períodos de variación legítima del tráfico, como entre los días de semana y los fines de semana.

La cuarta es el control de MFA: con el parámetro `zimbraFeatureTwoFactorAuthRequired` en Zimbra, era mejor habilitarlo en lugar de dejarlo como una opción (`zimbraFeatureTwoFactorAuthAvailable`), ya que la segunda alternativa dependía de que el usuario lo activara y ningún empleado lo hizo voluntariamente.

La quinta lección es sobre el panel de control con indicadores en tiempo real: cambió la idea del equipo de TIC sobre la seguridad institucional. Los empleados pasaron de ser ignorantes a estar conscientes de la situación porque podían ver los ataques en curso.

3.3.22 Ley Orgánica de Protección de Datos Personales (LOPDP)

La LOPDP, vigente en Ecuador desde el 26 de mayo de 2021, y su Reglamento General publicado el 13 de noviembre de 2023, establecieron el marco de obligaciones para el tratamiento de datos personales en instituciones públicas. Los principios de minimización de datos, limitación del propósito, exactitud, limitación del almacenamiento y seguridad resultan directamente aplicables al modelo de ciberresiliencia del GAD Salcedo, dado que el sistema de monitoreo procesa logs que pueden contener información personal de los ciudadanos que interactúan con los servicios digitales municipales.

El modelo implementó cuatro salvaguardas conforme a la LOPDP: la seudonimización de IPs internas en todas las representaciones públicas de los datos (los registros almacenados en OpenSearch conservan las IPs originales para fines operativos, pero las representaciones en documentos, dashboards compartidos y reportes utilizan identificadores anonimizados); la

limitación del propósito (los datos se procesan exclusivamente para detección de anomalías de seguridad, no para vigilancia de actividad individual de funcionarios); el acceso basado en roles (solo el equipo TIC autorizado accede al dashboard con datos completos); y la retención limitada (los logs se mantienen por un período máximo de 12 meses conforme a los requerimientos de auditoría del EGSI v3, tras lo cual se eliminan de forma segura).

3.3.23 Estado del Arte en Ciberresiliencia Municipal

La revisión sistemática de Hossain et al. (2024) describió que los gobiernos locales enfrentan un panorama de amenazas cada vez mayor con recursos relativamente decrecientes. Informaron que la inversión en ciberseguridad en los municipios de países en desarrollo es inferior al 2% del presupuesto total de TIC, en comparación con el 10-15% recomendado por los estándares internacionales. Estas brechas presupuestarias son una razón importante por la cual se seleccionan soluciones de código abierto como la implementada en GAD Salcedo.

Grothe et al. (2021) analizaron la implementación de marcos de seguridad en gobiernos locales de América Latina y concluyeron que los factores de éxito críticos fueron: el compromiso visible de la alta dirección (traducido en el comité de seguridad del modelo propuesto), la existencia de roles y responsabilidades formalizados (implementada mediante la Matriz RACI), y la medición continua de resultados mediante indicadores operativos (implementada mediante el dashboard de KPIs en OpenSearch Dashboards). Los autores enfatizaron que la tecnología por sí sola no produce mejoras sostenibles sin la articulación organizacional que la sostenga.

El informe ENISA Threat Landscape 2024 reportó un aumento del 35% en los ataques a instituciones gubernamentales europeas desde el año pasado, y el ransomware y la denegación de servicio fueron las principales amenazas (Agencia de la Unión Europea para la Ciberseguridad,

2024). Y aunque los datos provienen del sector europeo, esa tendencia también se observa en el sector público ecuatoriano. Esto se demuestra con los ataques documentados al municipio de Quito (ransomware BlackCat) y al propio GAD Salcedo (ataque coordinado de denegación de servicio + inundación SMTP en marzo de 2026).

3.3.24 Análisis del Log Viewer — Muestra en Tiempo Real

El archivo del Visor de Registros, que registró 150 eventos de firewall en un período de seis segundos durante el período de recopilación, proporcionó una perspectiva complementaria a nuestro análisis histórico. La distribución de eventos permitidos (114, equivalente al 76%) y eventos denegados (36, equivalente al 24%) indica una tasa de denegación anormalmente alta. En un firewall perimetral bien diseñado, esta proporción generalmente varía entre el 2% y el 5% del total bajo condiciones normales de operación.

Los eventos denegados se dividieron en tres categorías de tráfico malicioso. La primera, intentos de acceso desde IPs externas no autorizadas: la IP ucraniana 185.218.138.11 fue la más persistente con 6 intentos contra el puerto 4443 en 6 segundos. La segunda, fallos de autenticación de VPN: 3 intentos fallidos desde esa misma IP en 3 segundos; típicamente fuerza bruta. La tercera, tráfico interno no autorizado: solicitudes UDP al puerto 137 (Servicio de Nombres NetBIOS) y al puerto 3490, indicando actividad de difusión asociada con el reconocimiento de la red interna.

La regla de firewall con mayor actividad fue DNAT to Mail_Server, que canalizó el tráfico directo al servidor de correo Zimbra desde fuentes externas. Esta regla procesó tanto el tráfico legítimo de correo entrante como los intentos de ataque SMTP, lo que reforzó la decisión de incluir el servidor de correo como uno de los dos servicios críticos del piloto. La regla Default Deny

capturó todos los intentos de conexión que no coincidieron con ninguna regla permitida, y representó la principal fuente de eventos denegados.

3.3.25 Aplicaciones de Alto Riesgo Identificadas

El informe de Riesgos y Uso de Aplicaciones de Usuario de Sophos XGS3100 reveló cinco aplicaciones de riesgo nivel 4 y 5 desde la red interna de GAD Salcedo. Las aplicaciones de riesgo 5/5 son herramientas de túnel y evasión. Es probable que se utilicen como vectores para comunicar comando y control (C2) y exfiltración de datos. Las aplicaciones de riesgo 4/5 son clientes P2P, proxies y almacenamiento no corporativo, y pueden filtrar información de la empresa.

Basándonos en estos hallazgos, implementamos controles de aplicaciones con una política basada en el nivel de riesgo. Bloqueo inmediato para aplicaciones de riesgo 5/5 (túnel y evasión). Restricción con alerta para las de riesgo 4/5 (P2P y proxy). Política de uso aceptable documentada para las de riesgo 3/5. Los nombres de las aplicaciones fueron omitidos en este documento por razones de seguridad operativa de GAD Salcedo.

3.4 Impacto Organizacional del Modelo.

Además de los indicadores cuantitativos, la implementación del modelo proporcionó tres impactos organizacionales que se documentaron en entrevistas posteriores a la implementación. El primero fue una nueva conciencia situacional del equipo de TI. El equipo de TI nunca había tenido acceso al estado de seguridad de la infraestructura antes del modelo. El panel de control `GadSalcedo-Modelo1` proporcionó una vista en tiempo real de las tendencias, anomalías y amenazas activas, y evitó que el personal tuviera que verificar manualmente cada sistema cada día.

El segundo impacto fue la formalización de la comunicación de seguridad. La Matriz RACI llevó a canales claros de responsabilidad y notificación que no existían antes y con eso, se resolvió

la ambigüedad sobre quién debería actuar en respuesta a cada tipo de incidente. Las alertas automáticas que se envían por correo electrónico al Jefe de TI aseguraron que los eventos críticos fueran comunicados de inmediato, sin tener que pasar por la revisión manual del panel de control.

El tercer impacto fue la disponibilidad de evidencia auditable. El índice de incidentes de OpenSearch proporcionó un registro claro de cada incidente y tiempos detallados para su ocurrencia, detección y respuesta. Esta es una evidencia verificable para las auditorías de EGSI v3 y la rendición de cuentas ante las autoridades municipales. Antes del modelo, la institución no tenía un registro formal de incidentes de seguridad.

3.5 Análisis de Sostenibilidad.

La sostenibilidad del modelo se sustentó en tres cosas. La primera, costo de licencia cero: OpenSearch 2.19.5 es un software de código abierto sin tarifa de suscripción y se implementó en la infraestructura existente de Proxmox sin invertir en hardware adicional. El consumo de la máquina virtual `os-node1` (1% de CPU y 27% de RAM del nodo `srvmain2`) mostró que el modelo no compite por recursos de computación con los servicios en producción.

El segundo pilar estaba relacionado con la operación integrada dentro de las funciones ya realizadas por el equipo de TI. La Matriz RACI asigna la responsabilidad de monitorear, responder y mantener el modelo a los siete funcionarios según sus perfiles actuales, sin contratar a ningún otro personal ni asignar a nadie de manera exclusiva. Como hemos visto anteriormente, el reentrenamiento mensual del modelo y la revisión del tablero son actividades recurrentes en el ciclo operativo regular.

El tercer pilar fue la transferibilidad del modelo. La documentación completa del stack técnico (rsyslog + Python + OpenSearch), la configuración de los detectores RCF con parámetros

replicables y los manuales con procedimientos paso a paso abren la posibilidad para que otros GADs ecuatorianos con infraestructura Proxmox y firewall Sophos repliquen la solución con mínimas adaptaciones a su contexto. La comunidad de código abierto detrás de OpenSearch asegura el mantenimiento y las actualizaciones de la plataforma sin atar a la institución a ningún proveedor comercial.

CONCLUSIONES

En cuanto al primer objetivo específico, el diagnóstico de madurez del GAD Municipal de Salcedo tuvo un promedio de 1,0 sobre 5 en los nueve dominios evaluados por el EGSI v3. Tres estaban en el nivel 0 (inexistente): el comité de seguridad y gobernanza, la respuesta a incidentes y la medición de KPI. El cuestionario estructurado tipo Likert de 25 ítems tuvo un Alfa de Cronbach de $\alpha = 0,83$ y confirmó la consistencia interna del instrumento. Las entrevistas semiestructuradas confirmaron la opinión del equipo de TI: la amenaza era demasiado grande para los recursos actuales y los procesos para enfrentarlo. Se analizaron más de 8,3 millones de registros del Sophos XGS3100, acumulados desde noviembre de 2025, y se encontró una correlación de 95 456 ataques IPS en 24 horas y $r = 0,9991$ con la inundación de SMTP. Estos hallazgos confirmaron que la brecha no era tecnológica sino organizativa y procedimental.

Sobre el segundo objetivo específico, el modelo operativo se diseñó como una arquitectura de cuatro capas. La primera, gobernanza: Comité de Seguridad TIC, Matriz RACI con 7 roles y runbooks para 5 vectores de ataque. La segunda, monitoreo integrado: 8 índices en OpenSearch con más de 8,5 millones de documentos provenientes de tres fuentes (Sophos, Apache y Zimbra). La tercera, detección con IA: tres detectores Random Cut Forest con intervalo de 1 minuto, shingle_size 8, history 40 y reglas de supresión de falsos positivos. La cuarta, evaluación continua: sistema de KPIs con el dashboard GadSalcedo-Modelo1 en OpenSearch Dashboards. Como base normativa, el modelo se alineó con los marcos EGSI v3, NIST CSF 2.0, ISO 27001:2022 y AI RMF 1.0.

Para el tercer objetivo específico, el piloto se completó en la tercera semana de marzo de 2026. OpenSearch 2.19.5 se desplegó en la máquina virtual `os-node1` (Rocky Linux 9, IP

10.10.0.225, nodo `srvmain2` del clúster Proxmox). En este despliegue, se diseñaron siete canalizaciones de ingestión con rsyslog y scripts de Python, se configuraron tres detectores de anomalías basados en Random Cut Forest y se enviaron tres alertas al jefe de TI. Se utilizó autenticación multifactor para el 100% del equipo de TI (7/7 miembros del personal) con el parámetro `zimbraFeatureTwoFactorAuthRequired` en Zimbra.

Sobre el cuarto objetivo específico, la evaluación pre/post arrojó resultados estadísticamente significativos y operativamente contundentes. El MTTD cayó de 840 minutos la detección manual del incidente INC-001, previa a la activación de los detectores a 3 minutos en promedio (incidentes INC-003 e INC-004 detectados con la IA ya activa), una mejora del 99,6%. El MTTR pasó de 1 080 a 27 minutos, con una mejora del 97,5%. La tasa de falsos positivos quedó en 0% sobre los cuatro incidentes gestionados, por debajo de la meta establecida (menos del 15%). La MFA se incrementó de menos del 10% al 100% de las cuentas del equipo TIC. Los 1 225 fallos de autenticación detectados en Zimbra validaron la pertinencia de este control.

La detección automática del incidente INC-004 fuerza bruta IMAP a la cuenta fmarin@salcedo.gob.ec desde la IP 52.96.33.181 en 1 minuto con resolución en 14 minutos demostró que el modelo de IA cumple su propósito de detección temprana en un entorno municipal real. Sin el modelo, este incidente habría pasado desapercibido o habría sido detectado días después durante una revisión manual de logs, como ocurrió con el incidente INC-002 cuyo MTTD fue de 5.730 minutos.

La investigación demostró que el GAD Municipal de Salcedo transitó de un modelo reactivo sin capacidad de detección automatizada hacia un modelo proactivo basado en evidencia, con alertas en tiempo real, KPIs medibles y procesos documentados. El enfoque de código abierto

sobre infraestructura existente, sin inversión adicional en licencias ni hardware, constituye un aporte con alto potencial de transferibilidad al ecosistema de gobiernos locales ecuatorianos. El consumo de recursos de la VM de OpenSearch (1% de CPU y 27% de RAM del nodo `srvmain2`) confirmó que el modelo es sostenible sin afectar los servicios en producción.

RECOMENDACIONES

- Institucionalizar el Comité de Seguridad de la Información con reuniones mensuales documentadas y actas que sirvan de evidencia para auditorías EGSI v3, dado que la sostenibilidad del modelo depende del respaldo organizacional que el comité proporciona. Se recomienda que el Comité sea presidido por el Jefe de TIC con la participación de al menos un representante de la alta dirección del GAD.
- Mantener la MFA habilitada al 100% y extenderla progresivamente a las demás cuentas institucionales del GAD Salcedo, dado que los 1 225 fallos de autenticación documentados en Zimbra demuestran que los ataques de fuerza bruta son una amenaza activa y recurrente. Se recomienda priorizar las cuentas con acceso a información sensible (financiera, tributaria, recursos humanos).
- Implementar el bloqueo automatizado de IPs con clasificación de alto riesgo mediante la integración de feeds de threat intelligence (AbuseIPDB, Spamhaus) con las reglas del Sophos XGS3100, comenzando por la IP 185.218.138.11 que fue documentada con seis intentos de reconocimiento al puerto 4443.
- Establecer ventanas de parchado quincenales para los servidores críticos, con registro documentado del cumplimiento como evidencia del KPI de porcentaje de parchado definido en el modelo. Se recomienda priorizar las actualizaciones de seguridad de Apache, ModSecurity y Zimbra.
- Realizar el primer simulacro de respuesta ante incidentes dentro de los primeros 60 días de operación continua del modelo, utilizando el runbook de ataque DoS como escenario

base dado que fue el vector de mayor impacto documentado. Programar simulacros semestrales posteriores conforme a la Matriz RACI.

- Extender el modelo a los servicios adicionales del GAD Salcedo (DNS, base de datos, aplicaciones administrativas, Docker) en una segunda fase, una vez consolidados los resultados del piloto en correo y web. La extensión requiere la creación de nuevos índices en OpenSearch y la configuración de detectores RCF adicionales para cada servicio.
- Compartir los resultados con la Asociación de Municipalidades del Ecuador (AME) y la Coordinación de Ciberseguridad del MINTEL para contribuir al desarrollo de política pública en seguridad digital municipal. El modelo documentado con datos reales y métricas verificables puede servir como caso de referencia para otros GADs.
- Ejecutar el reentrenamiento mensual de los tres detectores RCF conforme al ciclo de gobierno del AI RMF 1.0, con revisión de los parámetros recency_emphasis y de las reglas de supresión para mantener la efectividad ante cambios en los patrones de tráfico institucional.
- Implementar un programa de capacitación en seguridad de la información para todo el personal del GAD, no solo el equipo TIC, dado que las entrevistas revelaron que los funcionarios administrativos desconocían las políticas de seguridad existentes y no habían recibido formación en buenas prácticas. Se recomienda al menos una sesión semestral con contenido adaptado al perfil de cada grupo.
- Documentar el proceso de implementación del modelo como un manual técnico replicable que incluya los scripts Python de ingesta, las configuraciones de rsyslog, los parámetros de los detectores RCF, los runbooks de respuesta y la configuración del

dashboard. Este manual facilitará la transferencia del modelo a otros GADs y la capacitación de nuevos miembros del equipo TIC.

REFERENCIAS

Borchert, O., Howell, G., Kerman, A., Rose, S., & Souppaya, M. (2025). *Implementing a Zero Trust Architecture: High-Level Document* (Número NIST SP 1800-35). https://doi.org/10.6028/NIST.SP.1800-35

Cybersecurity, & Agency, I. S. (2023). *Zero Trust Maturity Model Version 2.0*. https://www.cisa.gov/zero-trust-maturity-model

European Union Agency for Cybersecurity. (2024). *ENISA Threat Landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Grothe, M., del Rey, A., & Smith, J. (2021). Cyber security in local government. *Local Government Studies*, *47*(6), 977-996. https://doi.org/10.1080/03003930.2020.1866452

Hossain, S. T., Yigitcanlar, T., Xie, Y., & others. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences*, *14*(13), 5501. https://doi.org/10.3390/app14135501

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

Iturbe-Araya, I., Jiménez-Briseño, C., & others. (2025). Enhancing unsupervised anomaly-based cyberattacks detection. *International Journal of Information Security*, *24*(2), 1-22. https://doi.org/10.1007/s10207-024-00936-5

Lu, Y., Wang, J., & Zhao, H. (2023). Anomaly Detection in Data Streams. *Applied Sciences*, *13*(10), 6353. https://doi.org/10.3390/app13106353

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024a). *Instructivo para el control de avances del proyecto de implementación del EGSI*. https://www.gob.ec/sites/default/files/regulations/2024-08/1EG-como_presentar_informe_Control_de_Avances_EGSI.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024b). *Instructivo para la creación del proyecto EGSI v3*. https://www.gobiernoelectronico.gob.ec

National Institute of Standards, & Technology. (2023). *AI Risk Management Framework 1.0* (Número NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1

National Institute of Standards, & Technology. (2024). *NIST Cybersecurity Framework 2.0* (Número NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (Número NIST SP 800-207). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

ANEXOS

1. Anexo 1: Instrumento de Evaluación de Madurez EGSI v3

Encuesta de 25 ítems en 6 subescalas aplicada al equipo TIC (N = 7).

Ítem	Pregunta	Escala
GOV-1	¿Existe un comité formal de seguridad con reuniones periódicas?	0–1–2–3–4–5
GOV-2	¿Están definidos los roles y responsabilidades de seguridad?	0–1–2–3–4–5
GOV-3	¿Existe política de seguridad vigente y comunicada?	0–1–2–3–4–5
GOV-4	¿Se realizan reuniones periódicas con actas documentadas?	0–1–2–3–4–5
GOV-5	¿Existe plan de capacitación en seguridad?	0–1–2–3–4–5
IAM-1	¿Se aplica MFA en accesos a sistemas críticos?	0–1–2–3–4–5
IAM-2	¿Se revisan periódicamente los privilegios de acceso?	0–1–2–3–4–5
IAM-3	¿Se aplica el principio de mínimo privilegio?	0–1–2–3–4–5
IAM-4	¿Existe gestión del ciclo de vida de cuentas?	0–1–2–3–4–5
MON-1	¿Los logs son centralizados y revisados regularmente?	0–1–2–3–4–5
MON-2	¿Existen alertas automáticas para eventos anómalos?	0–1–2–3–4–5
MON-3	¿Se generan reportes periódicos de seguridad?	0–1–2–3–4–5
MON-4	¿Los logs son almacenados con protección contra alteración?	0–1–2–3–4–5
IR-1	¿Existen runbooks de respuesta ante incidentes?	0–1–2–3–4–5
IR-2	¿Se han realizado simulacros en el último año?	0–1–2–3–4–5
IR-3	¿Existe plan de comunicación para incidentes?	0–1–2–3–4–5
IR-4	¿Se documenta cada incidente con timestamps?	0–1–2–3–4–5

BCDR-1	¿Los respaldos son probados periódicamente?	0–1–2–3–4–5
BCDR-2	¿Están definidos RTO y RPO?	0–1–2–3–4–5
BCDR-3	¿Existe plan de continuidad documentado?	0–1–2–3–4–5
BCDR-4	¿Se realizan pruebas de restauración?	0–1–2–3–4–5
AIA-1	¿Existe detección automática de anomalías?	0–1–2–3–4–5
AIA-2	¿Se percibe valor en herramientas de detección automatizada?	0–1–2–3–4–5
AIA-3	¿Existe preocupación por privacidad en implementación de IA?	0–1–2–3–4–5
AIA-4	¿Se considera viable operar IA con el equipo actual?	0–1–2–3–4–5

Nota. Escala: 0=Inexistente, 1=Inicial, 2=Repetible, 3=Definido, 4=Gestionado, 5=Optimizado.

2. Anexo 2: Diccionario de KPIs Operativos

Diccionario de KPIs Operativos del Modelo

KPI	Definición	Fórmula	Frecuencia	Responsable
MTTD	Tiempo promedio detección	Σ(t_det–t_oc)/N	Mensual	Téc. Redes
MTTR	Tiempo promedio respuesta	Σ(t_resp–t_det)/N	Mensual	Jefe TIC
Disponibilidad	% tiempo operativo	(UP/Total)×100	Semanal	Téc. Sistemas
% MFA	Cuentas con MFA activa	(MFA/Total)×100	Mensual	Téc. Sistemas
% Parchado	Parches aplicados a tiempo	(Aplic./Prog.)×100	Quincenal	Téc. Sistemas

Tasa FP	Falsos positivos IA	(FP/Total)×100	Mensual	Téc. Redes

3. Anexo 3: Guía de Entrevista Semiestructurada

Guía para entrevistas individuales con los 7 miembros del equipo TIC.

Bloque 1: Conocimiento del EGSI v3

- ¿Conoce el EGSI v3?
- ¿Existe política de seguridad vigente?
- ¿Ha recibido capacitación en seguridad?

Bloque 2: Controles actuales

- ¿Cómo califica los controles actuales?
- ¿El Sophos XGS3100 es suficiente?
- ¿Qué aspectos necesitan más atención?

Bloque 3: Experiencias con incidentes

- ¿Ha experimentado incidentes de seguridad?
- ¿Cómo fue la respuesta institucional?
- ¿Cuánto tardó la detección y contención?

Bloque 4: Expectativas del modelo

- ¿Qué beneficios espera de la detección automatizada?
- ¿Qué preocupaciones tiene sobre IA?
- ¿Es viable operar el modelo con el equipo actual?

4. Anexo 4: Código de Configuración RCF en OpenSearch

Fragmento de la API REST para crear el detector Sophos-IPS-Anomaly-Detector.

```
PUT _plugins/_anomaly_detection/detectors
{
 "name": "Sophos-IPS-Anomaly-Detector",
 "description": "Deteccion de anomalias en trafico firewall GAD Salcedo",
 "time_field": "@timestamp",
 "indices": ["sophos-firewall"],
 "feature_attributes": [{
  "feature_name": "log_count",
  "feature_enabled": true,
  "aggregation_query": {"log_count": {"value_count": {"field": "_id"}}}
 }],
 "detection_interval": {"period": {"interval": 1, "unit": "Minutes"}},
 "shingle_size": 8,
 "rules": [{"action": "IGNORE_ANOMALY",
  "conditions": [

{"feature_name":"log_count","threshold_type":"ACTUAL_OVER_EXPECTED_RATIO
","value":0.2,"operator":"LTE"},

{"feature_name":"log_count","threshold_type":"EXPECTED_OVER_ACTUAL_RATIO
","value":0.2,"operator":"LTE"}
  ]}]
}
```

Nota. Configuración real extraída del detector activo ID Z5qGJZ0B6xocH5dskcj1 en OpenSearch 2.19.5, GAD Salcedo.

5. Anexo 5: Protocolo de Anonimización de Datos

- Sustitución de IPs internas por identificadores anonimizados en representaciones públicas.
- Eliminación de campos de usuario (usernames) antes del análisis estadístico.
- Truncamiento de marcas temporales a nivel de día en representaciones públicas.

El investigador declara que los datos fueron utilizados para fines académicos, con autorización de las autoridades del GAD Municipal de Salcedo, conforme a la LOPDP.