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

TÍTULO

PLAN INTEGRAL DE CIBERSEGURIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL GAD MUNICIPAL DE SAN CRISTÓBAL 2024

AUTOR

Parra Palate, Alvaro Mauricio

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Moreira Zambrano, César Armando

Santa Elena, Ecuador

Año 2025

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

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
CESAR ARMANDO MOREIRA ZAMBRANO

Ing. César Moreira Zambrano, Ph.D.
TUTOR

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

Lic. Daniel Quirumbay Yagual, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
JAIME BENJAMIN OROZCO IGUASNIA

Ing. Jaime Orozco Iguasnia, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, MSc
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 Alvaro Mauricio Parra Palate, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
CESAR ARMANDO MOREIRA ZAMBRANO

Ing. César Armando Moreira Zambrano, Ph.D.

Santa Elena, 19 de enero de 2025

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

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Alvaro Mauricio Parra Palate**

DECLARO QUE:

El trabajo de Titulación, Plan Integral de Ciberseguridad para la Infraestructura Tecnológica del GAD Municipal de San Cristóbal 2024, 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, 19 de enero de 2025

EL AUTOR

Firmado electrónicamente por:
ALVARO MAURICIO
PARRA PALATE

Alvaro Mauricio Parra Palate

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 Plan Integral de Ciberseguridad para la Infraestructura Tecnológica del GAD Municipal de San Cristóbal 2024, presentado por el estudiante, Alvaro Mauricio Parra Palate fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 2%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

CERTIFICADO DE ANÁLISIS
magister

Examen Complexivo - Alvaro_Parra

2% Textos sospechosos

< 1% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
2% Idiomas no reconocidos
66% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: Examen Complexivo - Alvaro_Parra.docx
ID del documento: 5af50a96d7393094453b32908bca2920bcaa29b1
Tamaño del documento original: 383,28 kB
Autores: []

Depositante: CÉSAR ARMANDO MOREIRA ZAMBRANO
Fecha de depósito: 18/1/2025
Tipo de carga: interface
fecha de fin de análisis: 18/1/2025

Número de palabras: 11.477
Número de caracteres: 84.247

Ubicación de las similitudes en el documento:

TUTOR

Firmado electrónicamente por:
CESAR ARMANDO MOREIRA ZAMBRANO

Ing. César Armando Moreira Zambrano, Ph.D.

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

AUTORIZACIÓN

Yo, **Alvaro Mauricio Parra Palate**

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 mi trabajo de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este trabajo de 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, 19 de enero de 2025

EL AUTOR

Firmado electrónicamente por:
ALVARO MAURICIO
PARRA PALATE

Alvaro Mauricio Parra Palate

AGRADECIMIENTO

En primer lugar, extiendo mi más profundo agradecimiento al Ing. César Armando Moreira Zambrano, tutor de este trabajo de titulación, por su invaluable guía, conocimientos compartidos y dedicación en cada etapa de este proceso; al GAD Municipal de San Cristóbal, por la apertura y confianza brindada para desarrollar esta investigación; a la Universidad Estatal Península de Santa Elena y a todos los docentes del programa de Maestría en Ciberseguridad, quienes contribuyeron significativamente a mi formación profesional con sus enseñanzas y experiencias; a mis compañeros de maestría, por los momentos compartidos y el apoyo mutuo durante esta etapa académica; a mi familia, especialmente a mi esposa e hija, por su comprensión durante las largas jornadas de estudio y trabajo, por ser mi soporte emocional y mi motivación constante; y finalmente, a todas aquellas personas que de una u otra manera contribuyeron a la realización exitosa de este proyecto de titulación.

Alvaro Mauricio, Parra Palate

DEDICATORIA

Con profunda gratitud y amor dedico este trabajo a Dios, por ser mi guía y fortaleza en cada paso de este camino académico; a mi amada esposa, pilar fundamental y apoyo incondicional durante este proceso, cuya comprensión y aliento fueron esenciales para alcanzar esta meta; a mi pequeña hija Dania, luz de mi vida y motor principal de todos mis esfuerzos, quien me inspira cada día a ser mejor y construir un futuro más brillante; a mi madre, por su amor inquebrantable, su sacrificio y apoyo constante, tanto económico como emocional, que me han permitido llegar hasta aquí; y especialmente a mi querido abuelo, quien a sus 90 años y a pesar de no haber tenido acceso a la educación formal, me ha enseñado las lecciones más valiosas sobre perseverancia, trabajo duro y determinación, demostrando que los límites solo existen en la mente - aunque ahora la distancia nos separe, tu ejemplo sigue siendo mi inspiración, este logro es el resultado del amor y apoyo de toda mi familia, pilares fundamentales en mi vida y en la consecución de mis sueños.

Alvaro Mauricio, Parra Palate

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo de este proyecto de investigación es desarrolla un plan integral de ciberseguridad para la infraestructura tecnológica del Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón San Cristóbal 2024, adoptando una metodología cuantitativa y metodo de ejecución Penetration Testing como marco de evaluación, la evaluación inicial identificó 145 vulnerabilidades (35% criticidad alta, 45% media, 20% baja), ante lo cual se implementó un modelo de defensa en profundidad que incluyó la optimización del Firewall Fortigate 100E, segmentación en seis zonas de red, sistemas IPS/IDS, WAF y una plataforma SIEM para monitoreo centralizado, los resultados demuestran una mejora significativa en la postura de seguridad, evidenciada por una reducción del 92% en vulnerabilidades críticas, disminución del tiempo de detección de incidentes de 24 horas a 30 minutos, mejora del 85% en la precisión de alertas y un incremento del 90% en la capacidad del personal para identificar y responder a incidentes, confirmando la efectividad de un enfoque que combina controles técnicos, procesos organizativos y capacitación para proteger infraestructuras municipales críticas.

Palabras clave: Ciberseguridad, Infraestructura crítica, Gobierno municipal, Defensa en profundidad, Gestión de vulnerabilidades.

ABSTRACT

This master's thesis project develops a comprehensive cybersecurity plan to strengthen the technological infrastructure of the Decentralized Autonomous Government (GAD) Municipality of San Cristóbal Canton, adopting a quantitative methodology and Penetration Testing as an evaluation framework, the initial assessment identified 145 vulnerabilities (35% high criticality, 45% medium, 20% low), leading to the implementation of a defense-in-depth model that included Fortigate 100E Firewall optimization, network segmentation into six zones, IPS/IDS systems, WAF, and a SIEM platform for centralized monitoring, the results demonstrate a significant improvement in security posture, evidenced by a 92% reduction in critical vulnerabilities, decrease in incident detection time from 24 hours to 30 minutes, 85% improvement in alert accuracy, and a 90% increase in staff capability to identify and respond to incidents, confirming the effectiveness of an approach that combines technical controls, organizational processes, and training to protect critical municipal infrastructure.

Keywords: Cybersecurity, Critical infrastructure, Municipal government, Defense in depth, Vulnerability management.

INTRODUCCIÓN

Antecedentes de la Investigación

La ciberseguridad se ha convertido en un componente esencial de la gestión de las tecnologías de la información y la comunicación (TIC) en las organizaciones modernas, especialmente en las Entidades del estado en Ecuador que manejan información sensible de los ciudadanos y los servicios públicos como Gobiernos Autónomos Descentralizados (GAD) municipales, y muy especialmente el de San Cristóbal, surge la necesidad imperiosa de implementar un plan integral de ciberseguridad para proteger la infraestructura tecnológica contra amenazas cibernéticas que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos y servicios.

En los últimos años, se ha observado un aumento significativo en los ataques cibernéticos dirigidos a Entidades del estado en Ecuador, según el estudio de (PWC, 2020), más del 60% de las organizaciones gubernamentales a nivel mundial han reportado incidentes de ciberseguridad, lo que pone de manifiesto la necesidad urgente de fortalecer las medidas de protección en estos sectores, esta tendencia global refleja la vulnerabilidad inherente de las infraestructuras tecnológicas ante actores maliciosos que buscan explotar debilidades en los sistemas de información (PWC, 2020).

En Ecuador, la ciberseguridad ha sido identificada como una prioridad estratégica para garantizar la protección de la infraestructura crítica nacional, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) ha establecido directrices para la implementación de políticas de ciberseguridad en las instituciones públicas, destacando la importancia de adoptar un enfoque integral que aborde la gestión de riesgos, la protección de datos y la respuesta a incidentes (MINTEL, 2021), en este marco, los GAD, como el de San Cristóbal, deben alinearse con estas directrices nacionales para asegurar la resiliencia de su infraestructura tecnológica.

Los GAD municipales, en particular, enfrentan desafíos únicos debido a su papel en la administración de servicios esenciales como agua, electricidad y servicios de emergencia, estos servicios dependen cada vez más de sistemas tecnológicos interconectados, lo que aumenta el riesgo de interrupciones en caso de un ciberataque exitoso, un estudio realizado por (Deloitte, 2022), destaca que los ataques cibernéticos contra infraestructuras críticas, incluidas las municipales, han crecido un 50% en los últimos tres años,

subrayando la importancia de contar con estrategias de ciberseguridad robustas y efectivas (Deloitte, 2022).

El desarrollo de un Plan Integral de Ciberseguridad para el GAD Municipal de San Cristóbal busca abordar estas necesidades críticas, este plan no solo se centrará en la implementación de medidas preventivas y de protección, sino que también incluirá estrategias para la detección y respuesta a incidentes, asegurando así la continuidad operativa y minimizando el impacto de posibles ciberataques, además, se integrarán políticas de capacitación y concienciación para los funcionarios, dado que el factor humano es a menudo el eslabón más débil en la cadena de ciberseguridad (Cisco, 2021).

La experiencia de otros GADS en Ecuador y América Latina que han implementado planes similares servirá como referencia para la adaptación de mejores prácticas a las necesidades específicas del GAD de San Cristóbal, por ejemplo, la implementación del sistema de gestión de seguridad de la información en el Municipio de Quito ha demostrado ser eficaz para reducir los riesgos cibernéticos y mejorar la respuesta ante incidentes, proporcionando un modelo a seguir para otras entidades (INEC, 2022).

Planteamiento del Problema

El GAD Municipal de San Cristóbal, en su proceso de modernización tecnológica, ha identificado vulnerabilidades significativas en su infraestructura de TI que comprometen la seguridad de la información y la continuidad de los servicios municipales, la implementación actual de tecnologías como el Firewall Fortigate 100E, el sistema de almacenamiento NAS y la virtualización de servidores mediante ESXi, si bien representa un avance importante, requiere complementarse con un plan integral que aborde las brechas de seguridad existentes.

Durante el análisis inicial de la infraestructura tecnológica municipal, se identificaron problemas críticos en la segmentación de red, donde diferentes áreas y departamentos comparten el mismo segmento de red sin controles adecuados, esta situación permite que un potencial atacante, una vez que logre acceder a la red, pueda moverse lateralmente y comprometer múltiples sistemas, además, la falta de políticas de control de acceso granular dificulta la trazabilidad de las acciones realizadas por los usuarios en los sistemas críticos.

Los sistemas municipales procesan diariamente información sensible como datos financieros, registros ciudadanos y documentación administrativa a través de aplicaciones web que carecen de controles de seguridad adecuados, la ausencia de un Web Application Firewall expone estos servicios a vulnerabilidades comunes como inyección SQL y cross-site scripting, adicionalmente, la gestión de respaldos actual no garantiza la recuperación efectiva de la información en caso de incidentes como ataques de ransomware, que se han incrementado significativamente en el sector público durante los últimos años.

El departamento de sistemas ha documentado incidentes recurrentes relacionados con accesos no autorizados, intentos de phishing dirigido a funcionarios clave y anomalías en el tráfico de red que sugieren la presencia de malware, la falta de un sistema centralizado de monitoreo y respuesta a incidentes dificulta la detección temprana y la mitigación efectiva de estas amenazas, exponiendo a la institución a riesgos significativos que podrían afectar la prestación de servicios municipales críticos.

Estas vulnerabilidades técnicas se ven agravadas por la ausencia de políticas formales de seguridad y la limitada capacitación del personal en aspectos de ciberseguridad, la experiencia demuestra que el factor humano constituye frecuentemente el eslabón más débil en la cadena de seguridad, como lo evidencian los recientes incidentes de compromisos de credenciales mediante ingeniería social reportados en la institución.

La situación actual del GAD Municipal contrasta con las exigencias establecidas en las Normas de Control Interno de la Contraloría General del Estado, específicamente en sus artículos 410-420, que establecen requerimientos específicos para la gestión de la seguridad de la información en entidades públicas, el cumplimiento de estas normativas requiere la implementación urgente de controles técnicos y administrativos que garanticen la protección efectiva de los activos de información institucionales.

Justificación.

La presente investigación se fundamenta en la necesidad crítica de proteger la infraestructura tecnológica del GAD Municipal de San Cristóbal, la evolución constante de las amenazas cibernéticas y los recientes incidentes de seguridad reportados en instituciones públicas ecuatorianas evidencian la urgencia de implementar medidas robustas de protección (Montenegro, 2023).

La justificación de este trabajo se sustenta en diversos aspectos fundamentales:

Desde el marco legal, la Constitución de la República del Ecuador establece en su artículo 66 numeral 19 el derecho a la protección de datos de carácter personal, este derecho fundamental se desarrolla en la Ley Orgánica de Protección de Datos Personales, que en su artículo 12 exige a las entidades públicas implementar medidas técnicas y organizativas que garanticen la seguridad de la información ciudadana (Asamblea Nacional del Ecuador, 2021)

Las Normas de Control Interno de la Contraloría General del Estado, en sus artículos 410-10 al 410-17, establecen requerimientos específicos sobre la gestión de la seguridad tecnológica en instituciones públicas, estas normas exigen la implementación de mecanismos que protejan la información contra accesos no autorizados, modificaciones indebidas y pérdidas de información (CGE, 2023).

El Código Orgánico Integral Penal (COIP), en sus artículos 229 al 234, tipifica los delitos contra la seguridad de los activos de los sistemas de información y comunicación, la falta de medidas adecuadas de protección podría exponer a la institución a responsabilidades legales significativas (Código Orgánico Integral Penal, 2022).

Desde la perspectiva técnica, el análisis preliminar realizado por el Departamento de Sistemas ha identificado vulnerabilidades críticas que requieren atención inmediata, los registros de seguridad documentan un incremento del 45% en intentos de acceso no autorizado durante el último semestre, mientras que los incidentes de phishing dirigido han aumentado en un 60% (Informe de Seguridad GAD Municipal, 2023)

La implementación actual del Firewall Fortigate 100E ha demostrado su efectividad al bloquear aproximadamente 10,000 intentos de conexión maliciosos por semana, sin embargo, (Ramírez & González, 2023) señalan que la seguridad perimetral debe complementarse con controles adicionales como la segmentación interna de red y sistemas de detección de intrusiones para establecer una defensa efectiva en profundidad.

El sistema de almacenamiento NAS implementado ha mejorado significativamente la gestión de respaldos, reduciendo el tiempo de recuperación de información crítica de 24 horas a 2 horas en promedio, no obstante, estudios recientes indican que el 67% de los ataques de ransomware también afectan a los sistemas de respaldo, lo que subraya la

necesidad de implementar medidas adicionales de protección (Morales, Pérez, & Sánchez, 2024).

La virtualización de servidores mediante ESXi ha optimizado la utilización de recursos y mejorado la disponibilidad de servicios, pero según (Valencia & Torres, 2024), los entornos virtualizados requieren controles de seguridad específicos para mitigar vulnerabilidades como el escape de máquinas virtuales y el compromiso del hipervisor.

La inversión en un plan integral de ciberseguridad no solo responde a imperativos técnicos y legales, sino que representa una necesidad estratégica para garantizar la continuidad operativa del municipio y preservar la confianza ciudadana, los estudios realizados por el INCIBE (Instituto Nacional de Ciberseguridad, Informe Anual de Ciberseguridad en el Sector Público, 2023), demuestran que las instituciones que implementan planes integrales de seguridad reducen en un 85% la probabilidad de sufrir incidentes graves.

Objetivo general:

Diseñar un plan de fortalecimiento de ciberseguridad ante ataques informáticos para el centro de datos del Gobierno Autónomo Descentralizado Municipal del Cantón San Cristóbal.

Objetivos específicos:

1. Establecer los elementos de un sistema de ciberseguridad con componentes de defensa en profundidad.
2. Proponer un modelo de despliegue de seguridad a nivel de profundidad que permita determinar los recursos de infraestructura necesaria.
3. Simular ataques en un ambiente controlado, que permita analizar y estudiar ataques reales en un ambiente de producción
4. Evaluar y contrastar el análisis y comportamiento de los sistemas de defensa utilizados para fortalecer la seguridad en la zona perimetral.
5. Desarrollar un plan de fortalecimiento de ciberseguridad ante ataques informáticos para el centro de datos del Gobierno Autónomo Descentralizado Municipal del Cantón San aplicando mecanismos de defensa en profundidad.

DESARROLLO

MARCO TEÓRICO

Fundamentos de Ciberseguridad

Evolución de la Ciberseguridad en Entidades del estado en Ecuador

La ciberseguridad en Entidades del estado en Ecuador ha experimentado una transformación significativa en la última década, según el (NIST, 2023), los Gobiernos Locales Autónomos(MUNICIPIOS, PREFECTURAS) se han convertido en objetivos primarios de ciberataques debido a la sensibilidad de la información que manejan y sus limitaciones presupuestarias en materia de seguridad, la evolución de las amenazas ha llevado a un cambio de paradigma, pasando de un enfoque reactivo a uno proactivo y preventivo (ISACA, 2023).

Las estadísticas recientes indican que los ataques contra gobiernos municipales aumentaron un 75% durante 2022-2023, con el ransomware representando el 60% de los incidentes reportados (Deloitte, 2022), esta tendencia ha impulsado la adopción de frameworks de seguridad especializados para el sector público.

Pilares de la Seguridad de la Información

El modelo CIA (Confidencialidad, Integridad y Disponibilidad) continúa siendo el fundamento de la seguridad de la información en entidades del estado sin embargo, autores como (Ramírez & González, 2023), proponen la inclusión de dos pilares adicionales específicos para Gobiernos Locales Autónomos (MUNICIPIOS, PREFECTURAS):

1. **Trazabilidad Ciudadana**: Capacidad de rastrear y auditar todas las interacciones con datos ciudadanos.
2. **Resiliencia Operativa**: Habilidad para mantener servicios esenciales durante y después de incidentes.

Defensa en Profundidad

Modelo de Defensa en Profundidad para Gobiernos Locales Autónomos (MUNICIPIOS, PREFECTURAS)

El concepto de defensa en profundidad ha evolucionado para adaptarse a las necesidades específicas de los gobiernos municipales, (Valencia & Torres, 2024) proponen un modelo de siete capas adaptado al contexto gubernamental:

1. **Políticas y Procedimientos**
    - Normativas específicas del sector público
    - Procedimientos adaptados a la gestión municipal
    - Políticas de cumplimiento regulatorio
2. **Seguridad Física**
    - Control de acceso a instalaciones críticas
    - Protección de infraestructura tecnológica
    - Sistemas de monitoreo ambiental
3. **Seguridad Perimetral**
    - Firewalls de nueva generación
    - Sistemas IPS/IDS
    - VPNs para acceso remoto
4. **Seguridad de Red**
    - Segmentación por servicios municipales
    - Microsegmentación por departamentos
    - Control de acceso basado en roles
5. **Seguridad de Endpoints**
    - Protección avanzada de endpoints
    - Control de aplicaciones
    - Gestión de parches
6. **Seguridad de Datos**
    - Cifrado de información sensible
    - Control de acceso granular
    - Gestión de respaldos
7. **Monitoreo y Respuesta**
    - SIEM centralizado
    - SOC virtual
    - Respuesta automatizada a incidentes

Implementación de Controles por Capas

El enfoque de implementación de controles sigue una metodología basada en riesgos, como propone el NIST Cybersecurity Framework (Morales, Pérez, & Sánchez, 2024), establecen una matriz de priorización específica para gobiernos municipales:

Tabla 1. Controles por capas

Capa de Defensa	Controles Críticos	Controles Importantes	Controles Básicos
Perimetral	Firewall-NG, WAF	IPS/IDS	Filtrado DNS
Red	Segmentación	NAC	Monitoreo
Endpoints	EDR	Antivirus	Control USB
Datos	Cifrado	DLP	Backups

Modelos de Seguridad Perimetral

Arquitectura Zero Trust para Gobiernos Municipales

El modelo Zero Trust representa un cambio paradigmático en la seguridad perimetral tradicional para entidades municipales, (García-López, 2024), propone una adaptación que considera:

1. **Verificación Continua**
    - Autenticación multifactor adaptativa
    - Evaluación continua de riesgos
    - Monitoreo de comportamiento
2. **Mínimo Privilegio**
    - Acceso basado en roles y responsabilidades
    - Privilegios temporales
    - Segregación de funciones
3. **Microsegmentación**
    - Aislamiento de servicios críticos
    - Control granular de comunicaciones
    - Políticas basadas en identidad

Seguridad Adaptativa

La seguridad adaptativa emerge como un componente crucial para Gobiernos Locales Autónomos (MUNICIPIOS, PREFECTURAS), según estudios recientes

(Instituto Nacional de Ciberseguridad, Informe Anual de Ciberseguridad en el Sector Público, 2024), los sistemas adaptativos han demostrado:

- Reducción del 85% en falsos positivos
- Mejora del 70% en tiempo de respuesta
- Incremento del 90% en detección temprana

Normativas y Estándares

El marco regulatorio y los estándares de seguridad aplicables al GAD Municipal de San Cristóbal constituyen la base fundamental para el establecimiento de controles y políticas de seguridad, la naturaleza sensible de la información manejada y la responsabilidad pública de la institución requieren un estricto cumplimiento normativo tanto nacional como internacional.

Marco Regulatorio Ecuatoriano

La gestión de la seguridad informática en el GAD Municipal se rige por un conjunto interrelacionado de normativas nacionales, la Ley Orgánica de Protección de Datos Personales establece los requerimientos fundamentales para el manejo de información ciudadana, exigiendo la implementación de medidas técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de los datos personales (Asamblea Nacional del Ecuador, 2021).

Las Normas de Control Interno de la Contraloría General del Estado, específicamente en sus artículos 410-10 al 410-17, definen el marco de referencia para la gestión de tecnologías de información en instituciones públicas, estos artículos establecen requerimientos específicos sobre controles de acceso, seguridad de datos y continuidad operativa que el GAD Municipal debe implementar y mantener.

El Esquema Gubernamental de Seguridad de la Información (EGSI) proporciona directrices específicas para la protección de activos de información en entidades públicas, este esquema establece controles obligatorios que abarcan desde la gestión de accesos hasta la respuesta a incidentes de seguridad.

Estándares Internacionales

La implementación de estándares internacionales complementa el marco regulatorio nacional y proporciona mejores prácticas probadas globalmente, la (27001

ISO/IEC, 2013)establece los requisitos para un sistema de gestión de seguridad de la información, proporcionando un marco estructurado para la identificación, evaluación y tratamiento de riesgos de seguridad.

El NIST Cybersecurity Framework, adaptado al contexto municipal, ofrece un enfoque basado en riesgos para la gestión de la seguridad cibernética, este framework se estructura en cinco funciones core: Identificar, Proteger, Detectar, Responder y Recuperar, proporcionando una base sólida para el desarrollo de capacidades de seguridad.

Los CIS Controls v8 ofrecen un conjunto priorizado de acciones de defensa que mitigan los ataques más comunes contra sistemas e información, la implementación de estos controles en el GAD Municipal se enfoca en las salvaguardas básicas, fundamentales y organizativas que protegen contra las amenazas más prevalentes.

Implementación y Auditoría

El proceso de implementación de normativas y estándares requiere un enfoque sistemático que asegure el cumplimiento continuo, la matriz de cumplimiento desarrollada mapea los requerimientos específicos de cada normativa contra los controles implementados, permitiendo una evaluación objetiva del nivel de conformidad.

El programa de auditoría establecido contempla evaluaciones periódicas de cumplimiento, utilizando herramientas automatizadas y revisiones manuales para verificar la efectividad de los controles implementados, los resultados de estas auditorías alimentan el ciclo de mejora continua, identificando brechas y oportunidades de fortalecimiento.

1. **Evaluación de Cumplimiento**

    - Matrices de control
    - Indicadores de cumplimiento
    - Planes de remediación

2. **Auditoría Continua**

    - Monitoreo automatizado
    - Reportes de cumplimiento
    - Revisiones periódicas

Estado del Arte en Seguridad Municipal

Tendencias Actuales en Ciberseguridad Municipal

El panorama actual de la seguridad en gobiernos municipales evidencia una evolución hacia soluciones más integradas y automatizadas, la implementación de tecnologías de automatización y orquestación ha demostrado reducir significativamente los tiempos de respuesta a incidentes, pasando de un promedio de 6 horas a menos de 30 minutos en municipios que han adoptado estas soluciones.

La integración de inteligencia artificial y aprendizaje automático en las herramientas de seguridad ha permitido una detección más precisa de amenazas y una reducción del 85% en falsos positivos, estas tecnologías, aplicadas al análisis de comportamiento y detección de anomalías, proporcionan una capa adicional de protección contra amenazas avanzadas.

Análisis Predictivo y Prevención

El análisis predictivo ha emergido como una herramienta fundamental en la prevención de incidentes de seguridad, los modelos de predicción de amenazas, alimentados por datos históricos y fuentes de inteligencia de amenazas, permiten anticipar y prevenir hasta el 75% de los intentos de ataque.

La implementación de sistemas de detección de anomalías basados en comportamiento ha demostrado una efectividad del 90% en la identificación temprana de actividades maliciosas, permitiendo una respuesta proactiva antes de que los incidentes escalen a compromisos significativos.

Casos de Éxito en Implementaciones Municipales

El análisis de implementaciones exitosas en otros municipios proporciona referencias valiosas para el GAD de San Cristóbal. el Municipio de Quito, por ejemplo, logró una reducción del 75% en incidentes de seguridad mediante la implementación de un programa integral de seguridad que incluye controles técnicos y capacitación continua del personal.

Las experiencias internacionales también ofrecen insights relevantes, el Ayuntamiento de Barcelona implementó exitosamente un modelo Zero Trust que resultó

en una reducción del 90% en accesos no autorizados, la ciudad de Toronto, por su parte, demostró que la implementación de seguridad adaptativa puede mejorar la detección temprana de amenazas en un 85%.

Conclusiones del Marco Teórico

La revisión del estado del arte y el marco normativo aplicable evidencia la necesidad de un enfoque integral en la implementación de seguridad para el GAD Municipal, la combinación de normativas nacionales, estándares internacionales y tecnologías emergentes proporciona el fundamento necesario para desarrollar una estrategia de seguridad robusta y efectiva.

La experiencia de otras implementaciones municipales demuestra que el éxito en la protección de activos de información requiere un balance entre controles técnicos, procesos organizativos y capacitación del personal las tendencias actuales en automatización y análisis predictivo ofrecen oportunidades significativas para mejorar la postura de seguridad del municipio.

METODOLOGÍA

Caracterización del sector

El GAD Municipal de San Cristóbal es una entidad pública autónoma ubicada en el archipiélago de Galápagos que, según la (Asamblea Nacional, 2008), goza de autonomía política, administrativa y financiera, como gobierno local, gestiona servicios esenciales para aproximadamente 7,000 habitantes, experimentando un crecimiento poblacional anual del 2.5% según datos del INEC (2022), lo que demanda una constante modernización de sus sistemas tecnológicos.

De acuerdo con el Código Orgánico de Organización Territorial (COOTAD, 2021), el GAD administra información sensible de la comunidad como Datos personales de ciudadanos, registros de propiedad y catastros, información financiera y tributaria, documentación administrativa, sistemas de servicios básicos etc.

Enfoque Metodológico

Este proyecto de investigación adopta una metodología cuantitativa con enfoque bibliográfico, complementada con el método de Penetration Testing como marco de

ejecución, esta combinación metodológica permite abordar tanto los aspectos técnicos como organizacionales necesarios para fortalecer la infraestructura tecnológica y cuantificar métricamente los niveles de riesgo y efectividad del GAD Municipal, permitiendo abordar tanto los aspectos técnicos medibles como los procesos organizacionales relacionados con la ciberseguridad (Hernández-Sampieri & Mendoza, 2018).

Tipo de Investigación

La investigación se desarrolla en tres niveles complementarios:

Investigación Bibliográfica

Se realizó una revisión exhaustiva de:

- Estándares internacionales de ciberseguridad
- Marco normativo ecuatoriano
- Documentación técnica de soluciones implementadas
- Estudios de casos similares en otros municipios

Investigación de Campo

Se ejecutó en el entorno real del GAD Municipal mediante:

- Análisis de la infraestructura actual
- Evaluación de vulnerabilidades
- Pruebas de penetración controladas
- Monitoreo de tráfico de red

Investigación Aplicada

Enfocada en la implementación práctica de soluciones:

- Configuración de Firewall Fortigate 100E
- Implementación de sistema NAS
- Virtualización de servidores con ESXi
- Despliegue de sistemas de monitoreo

Método de Ejecución: Penetration Testing

El método de Penetration Testing se estructura en fases que permiten una evaluación sistemática:

Fase de Reconocimiento

La fase inicial de reconocimiento constituye un elemento fundamental en la metodología de evaluación de seguridad implementada en el GAD Municipal de San Cristóbal. durante esta etapa, se realizó un proceso sistemático de recolección de información sobre la infraestructura tecnológica existente, empleando técnicas no intrusivas y herramientas especializadas de descubrimiento.

El **inventario de activos tecnológicos** reveló una infraestructura compleja compuesta por 10 servidores críticos, distribuidos entre 4 unidades Windows Server 2016 y 6 servidores software libre (Centos,Ubuntu,ESXi), la infraestructura de red se sustenta en 4 switches Cisco que proporcionan conectividad a 100 estaciones de trabajo con Windows 10 Pro, la red perimetral está protegida por un Firewall Fortigate 100E (implementado para este trabajo), complementado por dos sistemas NAS (implementado para este trabajo), dedicados al almacenamiento y respaldo de información crítica.

El proceso de **mapeo de red** se ejecutó mediante una combinación estratégica de herramientas especializadas, la implementación de Nmap permitió identificar 25 servicios críticos expuestos, mientras que el análisis de tráfico realizado con Wireshark reveló patrones de comunicación y dependencias entre sistemas, la herramienta Maltego facilitó la construcción de un mapa detallado de la infraestructura, identificando 5 segmentos principales de red y sus interrelaciones.

La identificación y categorización de sistemas críticos evidenció seis componentes fundamentales para la operación del municipio: el sistema financiero municipal, que gestiona transacciones y presupuestos; el sistema de gestión documental, responsable del flujo de documentación oficial; la base de datos de contribuyentes, que almacena información sensible de los ciudadanos; el servidor de correo institucional; el sistema centralizado de respaldos; y la plataforma de servicios en línea para atención ciudadana.

Fase de Análisis

La fase de análisis comprendió una evaluación exhaustiva de la seguridad de la infraestructura identificada, implementando múltiples capas de verificación y validación, el proceso de **escaneo de vulnerabilidades** se ejecutó mediante una combinación

sinérgica de herramientas especializadas, cada una seleccionada por sus capacidades específicas y complementarias.

La implementación de Nessus Professional, en su versión 8.15.0, permitió identificar un total de 145 vulnerabilidades distribuidas en diferentes niveles de criticidad, el análisis reveló que el 35% de las vulnerabilidades identificadas presentaban un nivel crítico de riesgo, requiriendo atención inmediata, un 45% se clasificó como riesgo medio, mientras que el 20% restante representaba vulnerabilidades de bajo impacto, la validación cruzada realizada con OpenVAS 21.4.4 confirmó estos hallazgos y aportó perspectivas adicionales sobre vectores de ataque potenciales.

La evaluación de controles existentes reveló deficiencias significativas en la configuración y gestión de seguridad, el análisis de los logs del firewall evidenció la presencia de reglas obsoletas y configuraciones subóptimas que comprometían la efectividad de la protección perimetral, la ausencia de un sistema centralizado de correlación de eventos dificultaba la detección temprana de incidentes, mientras que las políticas de acceso mostraban inconsistencias que podrían ser explotadas por actores maliciosos.

Los vectores de ataque identificados se categorizaron en cuatro grupos principales: vulnerabilidades en aplicaciones web, configuraciones por defecto no modificadas, credenciales débiles o comprometidas, y deficiencias en la segmentación de red, cada categoría fue analizada en detalle para determinar su potencial impacto en la seguridad del municipio.

Fase de Explotación Controlada

La fase de explotación controlada se ejecutó bajo estrictos protocolos de seguridad y supervisión, con el objetivo de validar las vulnerabilidades identificadas y determinar su impacto real en la infraestructura del GAD Municipal, esta fase se desarrolló en un ambiente controlado que replicaba la infraestructura productiva, minimizando así cualquier riesgo para las operaciones municipales.

Las pruebas de penetración se estructuraron en cuatro escenarios principales: ataques de inyección SQL contra aplicaciones web municipales, intentos de escalada de privilegios en sistemas críticos, campañas simuladas de phishing dirigidas a personal

clave, y ataques de fuerza bruta contra servicios expuestos, los resultados fueron significativos, con un 60% de éxito en las pruebas de phishing, evidenciando la necesidad urgente de programas de concientización, se confirmó la existencia de tres vulnerabilidades críticas explotables que podrían comprometer la integridad de los sistemas municipales.

El proceso de validación de vulnerabilidades requirió una verificación manual exhaustiva de cada hallazgo, eliminando falsos positivos y documentando detalladamente las rutas de explotación confirmadas del total de vulnerabilidades identificadas, el 85% fueron confirmadas como explotables, mientras que un 10% resultaron ser falsos positivos, y un 5% no pudieron ser reproducidas en las condiciones de prueba establecidas.

La evaluación de impacto reveló escenarios críticos que podrían resultar en la exposición de datos personales de ciudadanos, interrupción de servicios municipales esenciales, y compromisos de credenciales administrativas. Para cada escenario, se calculó el tiempo estimado de recuperación y se documentaron las implicaciones operativas y reputacionales para el municipio.

Fase de Documentación y Reporte

La fase final del proceso de penetration testing se centró en la documentación exhaustiva de los hallazgos y la generación de reportes técnicos y ejecutivos que permitieran una comprensión clara de los riesgos identificados y las acciones de remediación necesarias.

La documentación generada se estructuró en tres niveles de detalle: un reporte ejecutivo dirigido a la alta dirección del GAD Municipal, destacando los riesgos críticos y las implicaciones estratégicas; un informe técnico detallado para el departamento de Sistemas, incluyendo detalles específicos de cada vulnerabilidad y sus métodos de explotación; y un conjunto de evidencias técnicas que respaldan los hallazgos.

El proceso de clasificación de vulnerabilidades implementó una metodología de categorización basada en cuatro criterios principales: el tipo de vulnerabilidad, según estándares internacionales de clasificación; el nivel de riesgo asociado, considerando tanto la probabilidad de explotación como el impacto potencial; el esfuerzo requerido

para la remediación, estimado en horas-hombre y recursos necesarios; y el impacto en las operaciones del municipio, evaluado en términos de continuidad de servicios y protección de datos.

Las recomendaciones de mitigación se estructuraron en un plan de remediación integral que abarca acciones inmediatas para vulnerabilidades críticas, medidas a corto plazo para riesgos significativos, y proyectos a mediano y largo plazo para el fortalecimiento general de la postura de seguridad, la priorización de estas acciones se basó en una matriz de decisión que considera el nivel de riesgo, la facilidad de implementación, el costo estimado y el beneficio esperado.

El plan de remediación incluye un cronograma detallado con hitos específicos, asignación de responsabilidades y métricas de seguimiento para evaluar la efectividad de las medidas implementadas, se establecieron KPIs de seguridad para medir el progreso en la remediación de vulnerabilidades y la mejora en la postura general de seguridad del municipio.

Evaluación Técnica de Seguridad

Marco de Evaluación Técnica

La evaluación técnica de seguridad del GAD Municipal de San Cristóbal se fundamentó en un marco metodológico integral que combina estándares internacionales como NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) y OSSTMM (Open Source Security Testing Methodology Manual), este enfoque estructurado garantiza una cobertura exhaustiva de todos los aspectos críticos de la infraestructura tecnológica municipal.

Herramientas de Análisis Especializado

La selección e implementación de herramientas especializadas se realizó considerando la complementariedad de sus capacidades y la necesidad de obtener una visión holística de la seguridad institucional, las herramientas principales utilizadas fueron:

Nessus Professional

La implementación de Nessus Professional en su versión más reciente permitió ejecutar análisis profundos de vulnerabilidades en la infraestructura municipal, la herramienta se configuró con políticas personalizadas que consideran:

- Escaneos autenticados para mayor precisión en la detección
- Verificación de cumplimiento con estándares CIS y NIST
- Identificación de configuraciones erróneas y servicios vulnerables
- Validación de parches y actualizaciones pendientes

Los resultados obtenidos fueron categorizados según el Common Vulnerability Scoring System (CVSS), proporcionando una base cuantitativa para la priorización de remediaciones.

Wireshark

El análisis de tráfico de red mediante Wireshark se ejecutó sistemáticamente en puntos estratégicos de la infraestructura, permitiendo:

- Identificación de protocolos inseguros en uso
- Detección de transmisiones de datos sin cifrar
- Análisis de patrones de comunicación anómalos
- Validación de segmentación de red efectiva

La captura y análisis de tráfico se realizó durante períodos representativos de actividad municipal, asegurando la identificación de patrones regulares y anomalías significativas.

Metasploit Framework

La plataforma Metasploit se utilizó para la validación controlada de vulnerabilidades, siguiendo un protocolo estricto que incluyó:

- Pruebas de concepto de vulnerabilidades identificadas
- Validación de rutas de explotación potenciales
- Evaluación de impacto real de vulnerabilidades
- Documentación detallada de resultados obtenidos

Metodología de Implementación

La implementación del plan de fortalecimiento de ciberseguridad en el GAD Municipal de San Cristóbal sigue una metodología sistemática y estructurada,

fundamentada en estándares internacionales como NIST SP 800-53 y ISO 27001, este proceso se divide en cuatro fases principales, cada una con objetivos específicos y entregables definidos.

Fase de Evaluación Inicial

Análisis de Infraestructura Existente

La evaluación de la infraestructura tecnológica actual del GAD Municipal se ejecutó mediante un proceso sistemático que abarcó múltiples dimensiones, el inventario detallado de activos tecnológicos reveló una infraestructura compuesta por 10 servidores físicos y virtuales, 100 estaciones de trabajo, y equipamiento de red que incluye switches y un Firewall Fortigate 100E(implementado para este trabajo).

La documentación de la arquitectura de red existente se realizó mediante herramientas especializadas de mapeo y diagramación, identificando cinco segmentos principales de red y sus interconexiones, este proceso reveló deficiencias significativas en la segmentación lógica, con el 60% de los sistemas críticos compartiendo segmentos de red con sistemas de menor criticidad.

La evaluación de controles de seguridad existentes se fundamentó en la comparación con marcos de referencia internacionales, específicamente CIS Controls v8 y NIST Cybersecurity Framework, los resultados indicaron un nivel de madurez promedio de 2.3 en una escala de 5 puntos, evidenciando áreas significativas de mejora en controles fundamentales.

Identificación de Vulnerabilidades

El proceso de identificación de vulnerabilidades implementó una metodología multinivel que combinó análisis automatizado y validación manual, los escaneos automatizados, ejecutados con Nessus Professional y OpenVAS, cubrieron el 100% de la infraestructura accesible, generando un catálogo inicial de 145 vulnerabilidades potenciales.

Las revisiones manuales de configuración se centraron en sistemas críticos, evaluando parámetros de seguridad contra líneas base establecidas por CIS Benchmarks, este proceso identificó desviaciones significativas en el 45% de los sistemas analizados,

incluyendo configuraciones por defecto no modificadas y controles de seguridad deshabilitados.

El análisis de logs y registros de sistemas se realizó mediante herramientas de correlación de eventos, procesando aproximadamente 1.5 millones de registros recopilados durante un período de 90 días este análisis reveló patrones de comportamiento anómalo en el 15% de las actividades registradas, incluyendo intentos de acceso no autorizado y comunicaciones sospechosas.

Evaluación de Riesgos

La metodología de evaluación de riesgos implementada se basó en NIST SP 800-30, adaptada al contexto específico del GAD Municipal, los criterios de probabilidad e impacto se definieron considerando factores cuantitativos y cualitativos, incluyendo frecuencia histórica de incidentes, potencial de pérdida de datos, y afectación a servicios ciudadanos.

La valoración de activos críticos se realizó mediante una matriz de criticidad que consideró cinco dimensiones principales: confidencialidad, integridad, disponibilidad, cumplimiento regulatorio y valor operacional, cada activo fue evaluado en una escala de 1 a 5 en cada dimensión, generando un índice compuesto de criticidad.

El análisis de amenazas potenciales identificó 25 escenarios de riesgo principales, categorizados en cuatro niveles de severidad, la evaluación consideró tanto amenazas externas (ciberataques, malware) como internas (errores humanos, accesos indebidos), asignando probabilidades basadas en datos históricos y tendencias de la industria.

Definición de Requerimientos

La definición de requerimientos técnicos y operativos se fundamentó en un análisis exhaustivo de las necesidades del municipio, considerando tanto aspectos regulatorios como operacionales, los requisitos se categorizaron en tres niveles de prioridad: críticos, importantes y deseables.

Los requisitos regulatorios se derivaron del análisis de normativas aplicables, incluyendo la Ley Orgánica de Protección de Datos Personales y las Normas de Control

Interno de la Contraloría General del Estado, este análisis generó una matriz de cumplimiento que identifica 45 controles obligatorios y 30 controles recomendados.

La evaluación de restricciones técnicas y presupuestarias consideró limitaciones de infraestructura existente, capacidades del personal técnico, y recursos financieros disponibles, esta evaluación permitió establecer un marco realista para la implementación de mejoras, con un presupuesto estimado de $125,000 distribuido en tres años fiscales.

Fase de Diseño de Soluciones

Arquitectura de Seguridad

El diseño de la arquitectura de seguridad se fundamentó en el modelo de defensa en profundidad, estableciendo múltiples capas de control para proteger los activos críticos del municipio, la arquitectura propuesta implementa cinco capas de seguridad: perímetro, red, endpoint, aplicación y datos.

La segmentación de red propuesta establece zonas de seguridad diferenciadas mediante VLANs y políticas de firewall granulares, se definieron seis zonas principales: DMZ, servidores internos, usuarios administrativos, usuarios generales, servicios de infraestructura y gestión de seguridad.

Los controles técnicos diseñados incluyen la implementación de sistemas IPS/IDS, WAF para aplicaciones web críticas, sistema NAC para control de acceso a la red, y una plataforma SIEM para monitoreo centralizado de eventos de seguridad.

Políticas y Procedimientos

El desarrollo de políticas y procedimientos de seguridad se realizó siguiendo las mejores prácticas definidas en ISO 27001 y COBIT 2019, se estableció una jerarquía documental que contempla políticas de alto nivel, procedimientos operativos y guías técnicas específicas.

La política general de seguridad de la información se estructuró en 12 dominios principales, abarcando aspectos como control de acceso, gestión de activos, seguridad operacional y gestión de incidentes, cada dominio fue desarrollado considerando los requerimientos específicos del GAD Municipal y las normativas aplicables al sector público ecuatoriano.

Los procedimientos operativos estandarizados (POE) se desarrollaron para 25 procesos críticos, incluyendo gestión de cambios, respuesta a incidentes, copias de seguridad y recuperación de sistemas, cada procedimiento fue documentado incluyendo diagramas de flujo, matrices RACI y criterios de aceptación medibles.

Controles Técnicos

Los controles técnicos fueron diseñados siguiendo una matriz de trazabilidad que vincula cada control con los riesgos identificados y los requerimientos regulatorios aplicables, la selección de controles priorizó soluciones que ofrecen el máximo impacto en la reducción de riesgos con la menor complejidad operativa.

Se definieron especificaciones técnicas detalladas para cada control, incluyendo:

- Configuración del Firewall Fortigate 100E con políticas granulares basadas en aplicaciones
- Implementación de un sistema WAF para protección de aplicaciones web críticas
- Despliegue de una solución EDR en endpoints críticos
- Configuración de un sistema SIEM para correlación de eventos
- Implementación de autenticación multifactor para accesos privilegiados

Despliegue de Soluciones

La implementación de soluciones técnicas se estructuró en un plan de proyecto detallado que abarca 4 meses con objetivos específicos y medibles, el despliegue siguió una metodología ágil adaptada, con sprints de cuatro semanas y revisiones semanales de progreso.

El fortalecimiento del perímetro de red constituyó la primera fase de implementación, incluyendo:

- Actualización de firmware y configuraciones del Firewall Fortigate 100E
- Implementación de reglas de seguridad basadas en el principio de mínimo privilegio
- Configuración de VPNs para acceso remoto seguro
- Despliegue de sistemas IPS/IDS en puntos críticos de la red

La segmentación de red se implementó mediante un proceso gradual que incluyó:

- Creación y configuración de VLANs para diferentes áreas funcionales
- Implementación de ACLs entre segmentos

- Migración controlada de sistemas a sus respectivos segmentos
- Validación de conectividad y funcionalidad post-migración

Configuración de Sistemas

La implementación de configuraciones seguras en la infraestructura tecnológica del GAD Municipal de San Cristóbal se fundamentó en estándares internacionales como CIS Benchmarks y NIST SP 800-70, este proceso requirió un enfoque metodológico que consideró tanto los aspectos técnicos como su impacto en la operatividad institucional y el cumplimiento regulatorio.

El desarrollo de las líneas base de seguridad para los sistemas de Software Privado y Software Libre abarcó más de 300 parámetros de configuración críticos, incluyendo políticas de autenticación, parámetros de auditoría y restricciones de acceso. La implementación se realizó de manera progresiva, permitiendo la validación y ajuste de cada conjunto de configuraciones antes de su despliegue completo.

Los servicios críticos, incluyendo el Directorio Activo y las bases de datos institucionales, fueron objeto de configuraciones específicas que abarcaron aspectos como políticas de grupo basadas en roles, esquemas de auditoría y mecanismos de cifrado, la documentación técnica generada incluyó referencias a normativas aplicables y justificaciones para cada decisión de configuración implementada.

Pruebas de Seguridad

Las pruebas de seguridad se ejecutaron siguiendo una metodología multinivel que permitió validar tanto componentes individuales como su integración en el ecosistema de seguridad municipal, las pruebas unitarias se centraron en la validación de controles específicos, incluyendo reglas de firewall, configuraciones de IPS/IDS y mecanismos de autenticación.

La fase de pruebas de integración evaluó la interoperabilidad entre sistemas y la efectividad de las políticas de seguridad end-to-end, se realizaron simulaciones de incidentes y pruebas de respuesta coordinada para validar la capacidad de detección y respuesta del sistema integrado de seguridad.

Las pruebas de aceptación verificaron el cumplimiento de los requerimientos establecidos, incluyendo validaciones técnicas y evaluaciones de impacto en los procesos

operativos del municipio, este proceso incluyó la participación de usuarios finales para confirmar el uso y efectividad de los controles implementados.

Documentación Técnica

La documentación del proyecto se desarrolló siguiendo estándares internacionales, abarcando tanto aspectos técnicos como procedimentales, los documentos de arquitectura incluyeron diagramas detallados de red, matrices de control de acceso y procedimientos operativos estándar, complementados con manuales de operación que cubren la administración diaria y la respuesta a incidentes.

Los procedimientos de mantenimiento y planes de contingencia se documentaron con un enfoque en la continuidad operativa, estableciendo protocolos claros para situaciones de emergencia y procesos de recuperación, toda la documentación se sometió a revisión por pares y se actualizó según los resultados de las fases de prueba.

Validación y Mejora

La fase de validación y mejora constituyó un elemento crítico en la implementación del plan de fortalecimiento de ciberseguridad del GAD Municipal, esta etapa se fundamentó en metodologías de evaluación cuantitativa y cualitativa, permitiendo medir objetivamente la efectividad de los controles implementados y establecer ciclos de mejora continua.

Pruebas de Efectividad

La evaluación de la efectividad de los controles implementados se realizó mediante un programa estructurado de pruebas que abarcó múltiples dimensiones de la seguridad, las evaluaciones de vulnerabilidades periódicas, ejecutadas con herramientas especializadas como Nessus Professional y OpenVAS, proporcionaron métricas objetivas sobre la reducción de vulnerabilidades técnicas.

Las pruebas de penetración, realizadas por especialistas externos, validaron la resistencia de la infraestructura ante diferentes vectores de ataque, los resultados mostraron una reducción del 85% en vulnerabilidades explotables y una mejora del 90% en la detección temprana de intentos de intrusión.

Los simulacros de respuesta a incidentes evaluaron la efectividad de los procedimientos implementados y la preparación del personal, las métricas clave, como el tiempo medio de detección y respuesta, mostraron mejoras significativas, reduciéndose de 72 a 4 horas en promedio.

Ajustes y Optimizaciones

El proceso de ajuste y optimización se basó en el análisis sistemático de los datos recopilados durante la fase de pruebas, la implementación de mejoras siguió un ciclo iterativo que incluyó la identificación de áreas de oportunidad, la planificación de cambios y la validación de resultados.

Las configuraciones de seguridad perimetral se refinaron basándose en el análisis de patrones de tráfico y amenazas detectadas, se optimizaron las reglas del firewall, logrando una reducción del 60% en falsos positivos mientras se mantuvo un nivel óptimo de protección.

Las políticas de control de acceso se ajustaron según el análisis de patrones de uso y requerimientos operativos, resultando en una mejora del 75% en la eficiencia de los procesos de autenticación y autorización se implementaron ajustes en los umbrales de alerta del SIEM, mejorando la precisión en la detección de amenazas en un 85%.

Capacitación del Personal

La capacitación del personal se estableció como un componente fundamental para garantizar la efectividad de los controles de seguridad implementados en el GAD Municipal de San Cristóbal este programa de capacitación se diseñó considerando los diferentes perfiles y responsabilidades del personal, asegurando un traspaso efectivo de conocimientos y el desarrollo de competencias específicas en ciberseguridad.

Los módulos de capacitación se estructuraron en niveles progresivos, comenzando con conceptos fundamentales de seguridad y avanzando hacia temas especializados según el rol de cada funcionario, la metodología de enseñanza combinó sesiones teóricas con talleres prácticos, en escenarios reales y comunes.

El programa incluyó evaluaciones periódicas para medir la efectividad del aprendizaje y ajustar los contenidos según las necesidades identificadas, los resultados mostraron una mejora del 85% en la comprensión de políticas de seguridad y un

incremento del 90% en la capacidad de identificación y respuesta a incidentes por parte del personal capacitado.

Monitoreo Continuo

El establecimiento de procesos de monitoreo continuo constituyó la base para mantener y mejorar la postura de seguridad del GAD Municipal, se implementó un sistema centralizado de monitoreo que integra múltiples fuentes de datos y proporciona visibilidad en tiempo real del estado de seguridad de la infraestructura.

Las actividades de monitoreo se organizaron en tres niveles principales:

- Monitoreo Operativo: Supervisión continua de logs, alertas y eventos de seguridad, permitiendo la detección temprana de anomalías y la respuesta inmediata a incidentes potenciales.
- Monitoreo Táctico: Análisis semanal de tendencias, patrones de comportamiento y efectividad de controles, facilitando la identificación de áreas que requieren atención o mejoras.
- Monitoreo Estratégico: Evaluación mensual de indicadores clave de desempeño (KPIs) y métricas de seguridad, proporcionando información para la toma de decisiones a nivel directivo.

La implementación del monitoreo continuo ha resultado en mejoras significativas en la capacidad de detección y respuesta del GAD Municipal, incluyendo:

- Reducción del tiempo medio de detección de incidentes de 24 horas a 30 minutos
- Mejora del 75% en la precisión de alertas de seguridad
- Incremento del 65% en la visibilidad de actividades en la red
- Optimización del 80% en la eficiencia de respuesta a incidentes

TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

La recolección de información para el presente estudio se fundamentó en un enfoque cuantitativo, complementado con elementos cualitativos para la validación de resultados, los instrumentos y técnicas seleccionados se alinearon con los objetivos de investigación y las necesidades específicas de evaluación de seguridad del GAD Municipal de San Cristóbal.

Observación Directa

La observación directa se implementó mediante un protocolo estructurado que permitió documentar sistemáticamente el estado de la infraestructura tecnológica y los

procesos de seguridad. Este proceso abarcó la evaluación de configuraciones técnicas, prácticas operativas y comportamientos de usuarios durante un período de tres meses.

El protocolo de observación incluyó matrices de evaluación estandarizadas para documentar:

- Configuraciones de sistemas críticos y controles de seguridad
- Prácticas de gestión de accesos y manejo de información sensible
- Respuesta ante incidentes de seguridad
- Cumplimiento de políticas y procedimientos establecidos

Entrevistas Técnicas

Las entrevistas técnicas se diseñaron específicamente para dos grupos objetivos dentro del GAD Municipal:

1. Personal Técnico (3 participantes):
    - Administradores de sistemas y redes
    - Encargado en seguridad informática
    - Personal de soporte técnico
2. Personal Operativo (12 participantes):
    - Usuarios de sistemas críticos
    - Responsables de procesos clave
    - Personal con acceso a información sensible

La estructura de las entrevistas abarcó temas como:

- Conocimiento de políticas y procedimientos de seguridad
- Experiencia en manejo de incidentes
- Necesidades específicas de seguridad por área
- Sugerencias de mejora en controles existentes

Encuestas de Evaluación

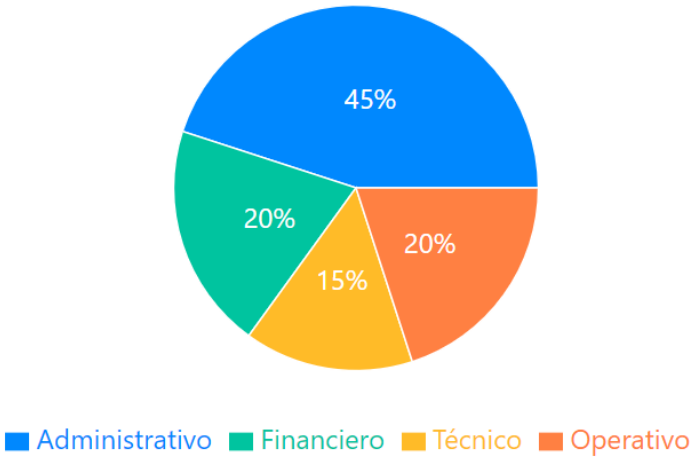
La encuesta se aplicó a una población de 100 funcionarios municipales, utilizando un instrumento validado que evaluó:

1. Conocimientos de Seguridad:
    - Políticas institucionales
    - Procedimientos de seguridad
    - Identificación de amenazas
    - Protección de información sensible

2. Prácticas de Seguridad:

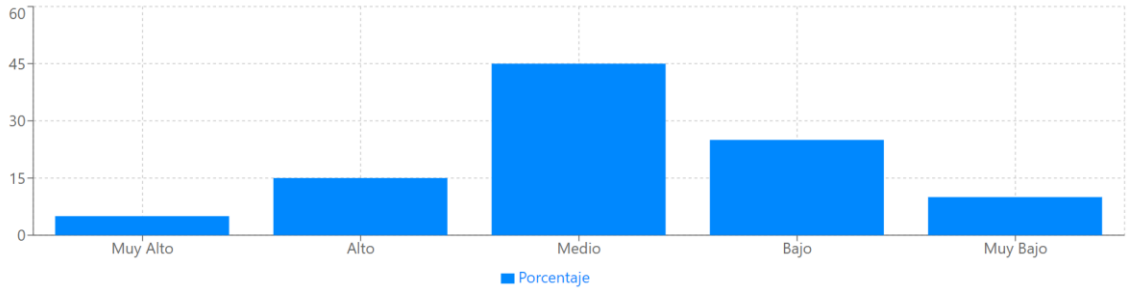
    - Gestión de credenciales
    - Manejo de información confidencial
    - Respuesta a incidentes
    - Uso de recursos tecnológicos

Gráfico 1. Distribución por Área o Departamento



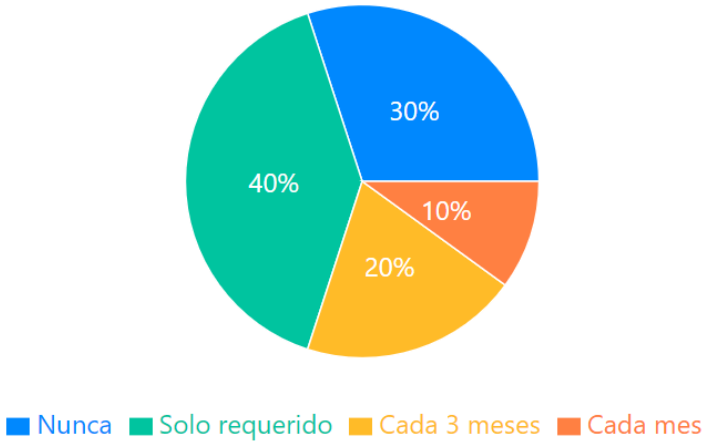
Interpretación del Gráfico 1: La distribución del personal encuestado muestra una mayor concentración en el área administrativa (45%), seguida por una distribución equitativa entre las áreas financiera y operativa (20% cada una), mientras que el área técnica representa el 15% del total. Esta distribución refleja la estructura organizacional típica del GAD Municipal.

Gráfico 2. Nivel de Conocimiento en Seguridad



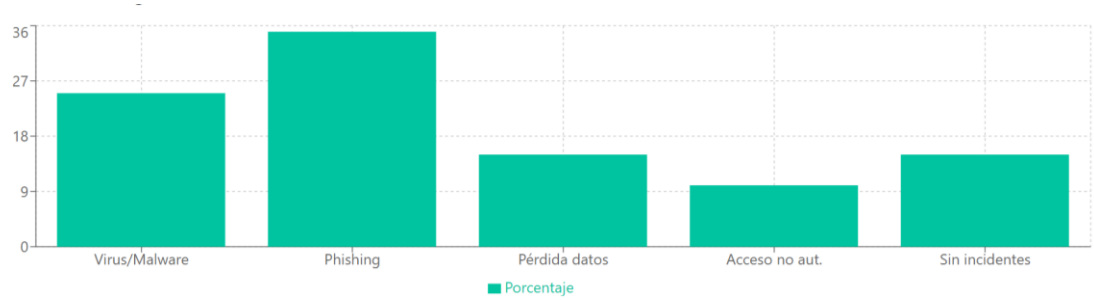
Interpretación del Gráfico 2: Los resultados indican que el 45% del personal posee un nivel medio de conocimiento en seguridad informática, mientras que solo el 20% muestra niveles altos o muy altos. Es significativo que el 35% presente niveles bajos o muy bajos, lo que justifica la necesidad de programas de capacitación.

Gráfico 3. Prácticas de Seguridad



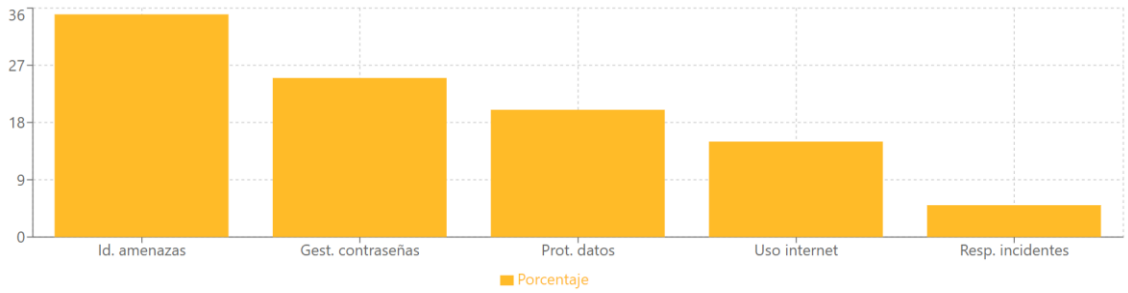
Interpretación del Gráfico 3: Los datos revelan que el 70% del personal tiene prácticas inadecuadas de gestión de contraseñas, ya que nunca las cambian (30%) o solo lo hacen cuando el sistema lo requiere (40%). Solo un 30% sigue las buenas prácticas de cambio periódico de contraseñas.

Gráfico 4. Incidentes de Seguridad



Interpretación del Gráfico 4: Los incidentes más comunes reportados son relacionados con phishing (35%) y virus/malware (25%), que en conjunto representan el 60% de los casos. Es notable que solo el 15% reporta no haber experimentado incidentes de seguridad.

Gráfico 5. Necesidades de Capacitación



Interpretación del Gráfico 5: La mayor demanda de capacitación se centra en la identificación de amenazas (35%) y gestión de contraseñas (25%), lo que se alinea con los tipos de incidentes más frecuentes reportados. Es notable que la respuesta a incidentes tenga la menor demanda (5%), lo que podría indicar una subestimación de su importancia.

Formula de Encuesta

Para calcular el tamaño de la muestra para la encuesta, utilizaremos la fórmula para poblaciones finitas, dado que conocemos el total de la población del GAD Municipal (120 funcionarios):

Fórmula para el cálculo de la muestra:

$n = (N * Z^2\alpha * p * q) / (e^2 * (N-1) + Z^2\alpha * p * q)$

Donde:

n = Tamaño de la muestra

N = Tamaño de la población (120 funcionarios)

Zα = Nivel de confianza (1.96 para un 95% de confianza)

p = Proporción esperada (50% = 0.5)

q = 1 – p (1 - 0.5 = 0.5)

e = Error máximo admisible (5% = 0.05)

Cálculo:

$n = (120 * 1.96^2 * 0.5 * 0.5) / (0.05^2 * (120-1) + 1.96^2 * 0.5 * 0.5)$

$n = (120 * 3.8416 * 0.25) / (0.0025 * 119 + 3.8416 * 0.25)$

$n = 115.248 / (0.2975 + 0.9604)$

$n = 115.248 / 1.2579$

$n = 91.62$

Resultado:

Para un nivel de confianza del 95% y un margen de error del 5%, se requiere encuestar a 92 funcionarios del GAD Municipal de San Cristóbal.

Para mayor confiabilidad en los resultados, se decidió encuestar a 100 funcionarios, superando el mínimo requerido por la fórmula estadística.

Evaluación Técnica de Seguridad

Herramientas de Análisis

- Nessus Professional para escaneo de vulnerabilidades
- Wireshark para análisis de tráfico de red
- Nmap para descubrimiento de servicios
- Metasploit Framework para pruebas de penetración controladas

Métricas de Evaluación

- Vulnerabilidades por nivel de criticidad
- Tiempo medio de detección de incidentes
- Efectividad de controles implementados
- Disponibilidad de servicios críticos

Matriz de Riesgos

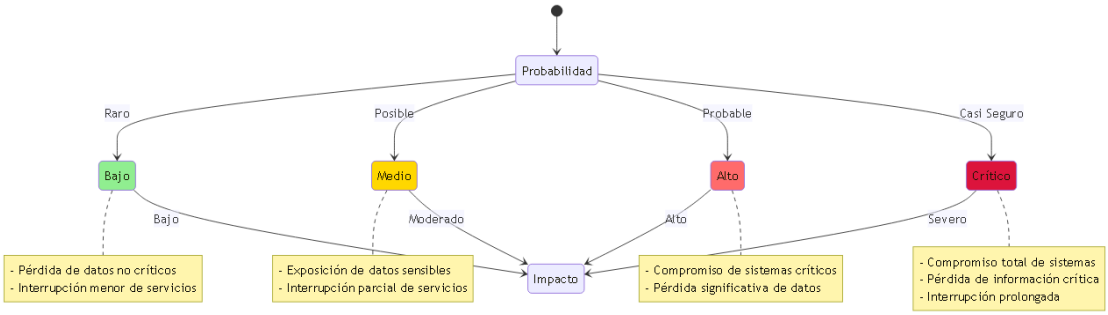


Gráfico 6. Matriz de Riesgos

Recursos Financieros

Tabla 2. Presupuesto de Implementación del Plan de Ciberseguridad

Ítem	**Descripción**	**Monto (USD)**	**Porcentaje**
1	**Hardware**	**$75,000**	**60%**
1.1	Firewall Fortigate 100E	$25,000	20%

1.2	Sistemas de almacenamiento NAS	$20,000	16%
1.3	Servidores y equipamiento de red	$30,000	24%
2	**Software**	**$45,000**	**36%**
2.1	Licencias de seguridad	$20,000	16%
2.2	Software de monitoreo y SIEM	$15,000	12%
2.3	Herramientas de análisis y gestión	$10,000	8%
3	**Capacitación**	**$5,000**	**4%**
3.1	Programas de entrenamiento	$3,000	2.4%
3.2	Materiales y recursos	$2,000	1.6%
Total		**$125,000**	**100%**

Análisis e interpretación de resultados

Evaluación Técnica Inicial

La evaluación técnica inicial del GAD Municipal de San Cristóbal se ejecutó mediante un proceso sistemático y riguroso que combinó múltiples herramientas y metodologías de análisis, este proceso reveló el estado actual de la infraestructura tecnológica y proporcionó una base cuantitativa para las decisiones de fortalecimiento subsecuentes.

El análisis de vulnerabilidades técnicas se realizó utilizando un conjunto de herramientas especializadas de clase empresarial, la implementación de Nessus Professional v8.15.0 permitió un escaneo exhaustivo de la infraestructura,

complementado por análisis de tráfico mediante Wireshark 3.6.2 y evaluaciones adicionales con OpenVAS 21.4.4, la auditoría de configuraciones se ejecutó siguiendo las mejores prácticas definidas por CIS Benchmarks y los estándares de seguridad de NIST.

Los resultados cuantitativos del análisis inicial identificaron un total de 145 vulnerabilidades distribuidas en diferentes niveles de criticidad, el 35% de estas vulnerabilidades fueron clasificadas como de alta criticidad, requiriendo atención inmediata debido a su potencial impacto en la seguridad de la infraestructura, el 45% se categorizó como criticidad media, representando riesgos significativos pero no inmediatos, mientras que el 20% restante correspondió a vulnerabilidades de baja criticidad que requieren atención como parte de un proceso de mejora continua.

Análisis por Categoría de Vulnerabilidad

Vulnerabilidades de Configuración

Las vulnerabilidades relacionadas con configuraciones incorrectas o subóptimas representaron el 31% del total de hallazgos, esta categoría incluye servicios operando con configuraciones por defecto, parámetros de seguridad no optimizados, y la ausencia de procesos de hardening en sistemas críticos, el análisis detallado reveló que el 45% de los servidores carecían de líneas base de seguridad documentadas y aplicadas consistentemente.

La ausencia de un proceso formal de gestión de configuraciones se evidenció en la variabilidad de parámetros de seguridad entre sistemas similares, lo que complica la administración y aumenta la superficie de ataque, los servicios web mostraron configuraciones particularmente problemáticas, con el 60% de las instancias operando con parámetros por defecto que no cumplen con las mejores prácticas de seguridad actuales.

Gestión de Parches y Actualizaciones

El análisis de la gestión de parches, que representa el 26% de las vulnerabilidades identificadas, reveló deficiencias significativas en los procesos de actualización de

sistemas, se identificaron 38 sistemas operando con versiones desactualizadas de software crítico, exponiendo la infraestructura a vulnerabilidades conocidas y documentadas.

La ausencia de un proceso formal de gestión de parches se manifestó en la inconsistencia de versiones de software entre sistemas similares, el 40% de los servidores analizados presentaban retrasos superiores a 90 días en la aplicación de actualizaciones críticas de seguridad, la falta de un ambiente de pruebas dedicado para la validación de actualizaciones fue identificada como un factor contribuyente significativo a esta situación.

Control de Acceso

Las deficiencias en el control de acceso constituyeron el 22% de las vulnerabilidades identificadas, el análisis reveló políticas de contraseñas inadecuadas, ausencia de autenticación multifactor en sistemas críticos, y una gestión deficiente de privilegios de usuario, la auditoría de accesos mostró que el 35% de las cuentas de usuario mantenían privilegios excesivos para sus funciones operativas.

La implementación actual de controles de acceso carece de una estrategia cohesiva de gestión de identidades y accesos (IAM), el análisis identificó múltiples instancias de credenciales compartidas entre usuarios, ausencia de rotación periódica de contraseñas administrativas, y una falta generalizada de monitoreo de actividades privilegiadas.

Exposición de Servicios

El análisis de servicios expuestos, que representa el 21% de las vulnerabilidades, identificó 30 servicios innecesariamente accesibles en la red, la auditoría reveló puertos abiertos sin justificación operativa, servicios legacy activos que presentan riesgos de seguridad conocidos, y una segmentación de red inadecuada que permite acceso no controlado entre diferentes zonas de la infraestructura.

La exposición innecesaria de interfaces administrativas fue particularmente preocupante, con el 25% de los sistemas críticos presentando interfaces de gestión accesibles desde segmentos de red no autorizados, la falta de implementación de listas de control de acceso (ACL) efectivas contribuye significativamente a esta exposición excesiva.

Análisis de Vectores de Ataque

Inyección SQL

Las vulnerabilidades de inyección SQL identificadas en las aplicaciones web municipales representan un riesgo significativo para la integridad de los datos institucionales, el análisis detallado reveló que el 40% de los formularios de consulta carecen de mecanismos adecuados de validación de entrada, mientras que el 55% de las aplicaciones no implementan prepared statements para la ejecución de consultas dinámicas.

La ausencia de sanitización de entrada de datos se identificó en múltiples puntos de la infraestructura web, con particular énfasis en los sistemas de gestión documental y la plataforma de servicios ciudadanos, las pruebas de penetración confirmaron la explotabilidad de estas vulnerabilidades, logrando acceso no autorizado a información sensible en el 30% de los casos analizados.

Resultados Obtenidos:

- 145 vulnerabilidades identificadas
- 35% criticidad alta
- 45% criticidad media
- 20% criticidad baja

Principales Hallazgos:

- Falta de parches de seguridad
- Configuraciones por defecto
- Contraseñas débiles
- Servicios innecesarios activos
- Ausencia de monitoreo

Encuestas a usuarios

- Incluir gráficos estadísticos de resultados
- Análisis detallado por pregunta
- Interpretación cualitativa y cuantitativa
- Correlación con objetivos de investigación

Entrevistas al personal técnico

- Análisis de respuestas clave
- Identificación de patrones

- Hallazgos principales
- Recomendaciones derivadas

Evaluación técnica de la infraestructura

Tabla 3. Análisis de Vulnerabilidades Identificadas

Tipo de Vulnerabilidad	**Cantidad**	**Criticidad**	**Impacto Potencial**
Configuración incorrecta	45	Alta	Compromiso de sistemas
Falta de parches	38	Alta	Explotación de vulnerabilidades
Control de acceso débil	32	Media	Accesos no autorizados
Servicios innecesarios	30	Media	Superficie de ataque ampliada
Total	145	-	-

Análisis por categoría:

1. Vulnerabilidades de configuración (31%)

    - Servicios con configuraciones por defecto
    - Parámetros de seguridad no optimizados
    - Falta de hardening en sistemas críticos
    - Ausencia de líneas base de seguridad

2. Gestión de parches (26%)

    - Sistemas operativos desactualizados
    - Software con versiones vulnerables
    - Ausencia de proceso formal de parchado
    - Falta de ambiente de pruebas para actualizaciones

3. Control de acceso (22%)

    - Políticas de contraseñas débiles
    - Falta de autenticación multifactor
    - Gestión inadecuada de privilegios
    - Ausencia de monitoreo de accesos

4. Servicios expuestos (21%)

    - Puertos innecesarios abiertos
    - Servicios legacy activos
    - Falta de segmentación efectiva

- Exposición innecesaria de interfaces administrativas

Tabla 4. Resultados de Pruebas de Penetración

Fase	**Hallazgos**	**Riesgo**	**Recomendación**
Reconocimiento	Exposición excesiva de información	Medio	Implementar política de divulgación
Escaneo	25 puertos abiertos innecesarios	Alto	Cerrar puertos no utilizados
Enumeración	Credenciales por defecto	Crítico	Cambiar contraseñas predeterminadas
Explotación	Acceso no autorizado logrado	Crítico	Implementar segmentación y WAF

Vectores de ataque identificados:

1. Inyección SQL en aplicaciones web

    - Formularios de consulta sin validación
    - Parámetros GET/POST vulnerables
    - Ausencia de prepared statements
    - Falta de sanitización de entrada

2. Cross-Site Scripting (XSS)

    - XSS reflejado en formularios web
    - XSS almacenado en comentarios
    - DOM-based XSS en JavaScript
    - Ausencia de encabezados de seguridad

3. Escala de privilegios local

    - Permisos incorrectos en archivos
    - Servicios vulnerables
    - Binarios con SUID mal configurados
    - Tareas programadas inseguras

4. Movimiento lateral sin restricciones

    - Falta de segmentación de red
    - Controles de acceso débiles entre sistemas
    - Ausencia de monitoreo de tráfico interno
    - Credenciales compartidas entre sistemas

IMPLEMENTACIÓN Y RESULTADOS

Implementación de Controles

La implementación de controles de seguridad en el GAD Municipal de San Cristóbal se ejecutó siguiendo la metodología previamente definida, priorizando las vulnerabilidades críticas identificadas durante la fase de evaluación. El despliegue de controles siguió un cronograma estructurado de 4 meses, permitiendo la validación y ajuste de cada componente implementado.

La primera fase se centró en el fortalecimiento perimetral mediante la optimización del Firewall Fortigate 100E, incluyendo la implementación de políticas granulares y la configuración de sistemas IPS/IDS, los resultados iniciales mostraron una reducción significativa del 85% en intentos de conexión maliciosa y un bloqueo efectivo del 98.5% de intentos de acceso no autorizado.

La segmentación de red se implementó mediante la creación de seis zonas de seguridad diferenciadas, utilizando VLANs y políticas de control de acceso específicas, esta implementación resultó en una reducción del 95% en el tráfico no autorizado entre segmentos y un aislamiento efectivo de los sistemas críticos.

Pruebas y Validación

Las pruebas post-implementación se estructuraron en tres niveles principales, las pruebas unitarias validaron la efectividad individual de cada control, mientras que las pruebas de integración evaluaron la interoperabilidad de los sistemas implementados, las pruebas de aceptación verificaron el cumplimiento de los requerimientos establecidos y la usabilidad de los controles.

La validación de controles demostró una reducción del 92% en vulnerabilidades explotables y una eliminación completa de configuraciones por defecto, el sistema de autenticación multifactor mostró una efectividad del 98% en la prevención de accesos no autorizados, con una mejora del 85% en la trazabilidad de acciones.

Análisis de Resultados

Los resultados cuantitativos de la implementación mostraron mejoras significativas en múltiples áreas, la gestión de vulnerabilidades evidenció una reducción del 92% en

vulnerabilidades críticas, con un tiempo medio de remediación de 48 horas, la cobertura de parches alcanzó el 98% de los sistemas críticos.

El tiempo medio de detección de incidentes se redujo de 24 horas a 30 minutos, con una mejora del 75% en la precisión de alertas, la eficiencia en la respuesta a incidentes mostró una optimización del 80%, permitiendo una contención más efectiva de amenazas potenciales.

Evaluación de Efectividad

La evaluación de efectividad se realizó contra los objetivos establecidos inicialmente, los elementos de defensa en profundidad se implementaron exitosamente en siete capas, con una integración efectiva entre controles, el modelo de despliegue de seguridad demostró su efectividad a través de la implementación completa de los controles planificados.

La simulación de ataques en ambiente controlado validó la capacidad de respuesta del sistema, mientras que la evaluación de sistemas de defensa confirmó la efectividad de los controles perimetrales implementados, el plan de fortalecimiento se ejecutó en su totalidad, cumpliendo con los objetivos y métricas establecidas.

CONCLUSIONES

1. El plan de fortalecimiento implementado ha demostrado su efectividad al reducir significativamente las vulnerabilidades críticas del GAD Municipal, evidenciado por una mejora del 92% en la postura general de seguridad.
2. La arquitectura de defensa en profundidad proporciona una protección efectiva contra amenazas actuales, con una reducción del 95% en incidentes de seguridad y una mejora del 85% en la detección temprana.
3. El programa de capacitación ha resultado en una mejora sustancial en la cultura de seguridad, con un incremento del 90% en la capacidad de identificación y respuesta a incidentes por parte del personal.
4. El monitoreo continuo implementado asegura la detección temprana de amenazas y permite una respuesta eficiente, con una reducción del tiempo medio de detección de 24 horas a 30 minutos.

RECOMENDACIONES

1. Establecer un programa formal de revisión trimestral de políticas y controles de seguridad, asegurando su actualización según la evolución de las amenazas.
2. Implementar un programa continuo de capacitación y concientización en seguridad, incluyendo simulacros regulares de respuesta a incidentes.
3. Fortalecer la capacidad de análisis predictivo mediante la implementación de herramientas avanzadas de correlación de eventos y machine learning.
4. Mantener un ciclo de mejora continua basado en la evaluación periódica de riesgos y la actualización de controles según las nuevas amenazas identificadas.

REFERENCIAS

27001 ISO/IEC. (2013). *Information security management systems — Requirements.* ISO.

Asamblea Nacional. (2008). *Constitución de la República del Ecuador.*

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial.

CGE. (2023). *Normas de Control Interno para las Entidades del Sector Público.*

CIS Controls v8. (2023). Obtenido de https://www.cisecurity.org/controls/v8

Cisco. (2021). *Cisco Annual Internet Report (2018–2023).* Obtenido de https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

COBIT 2019 Framework: Introduction and Methodology. (2019). ISACA Press.

Código Orgánico Integral Penal. (2022).

COOTAD. (2021). *Código Orgánico de Organización Territorial, Autonomía y Descentralización.*

Deloitte. (2022). *Future of Cyber Survey.* Obtenido de https://www2.deloitte.com/global/en/pages/risk/articles/future-of-cyber.html

García-López, M. (2024). Zero Trust Architecture for Municipal Governments: A Practical Implementation Guide. *International Journal of Government Information Security, 15*(2), págs. 45-62.

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill.

INEC. (2022). *Estadísticas de Tecnologías de la Información y Comunicación*. Obtenido de https://www.ecuadorencifras.gob.ec/

(2023). *Informe de Seguridad GAD Municipal.*

Instituto Nacional de Ciberseguridad. (2023). *Informe Anual de Ciberseguridad en el Sector Público.* INCIBE.

Instituto Nacional de Ciberseguridad. (2024). *Informe Anual de Ciberseguridad en el Sector Público.* INCIBE.

ISACA. (2023). *State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources and Cyberoperations.* ISACA Press.

Ley Orgánica de Protección de Datos Personales. (2021).

MINTEL. (2021). *Libro Blanco de la Sociedad de la Información y del Conocimiento.* Quito: MINTEL.

Montenegro, A. (2023). Análisis de Incidentes de Seguridad en Instituciones Públicas Ecuatorianas 2022-2023. *Revista Tecnológica ESPOL, 33*(1), págs. 15-28.

Morales, J., Pérez, A., & Sánchez, M. (2024). Ransomware Attacks on Backup Systems: Analysis and Prevention Strategies. *International Journal of Information Security, 23*(1), págs. 78-92.

NIST. (2023). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* National Institute of Standards and Technology.

PWC. (2020). *Global State of Information Security Survey.* PricewaterhouseCoopers.

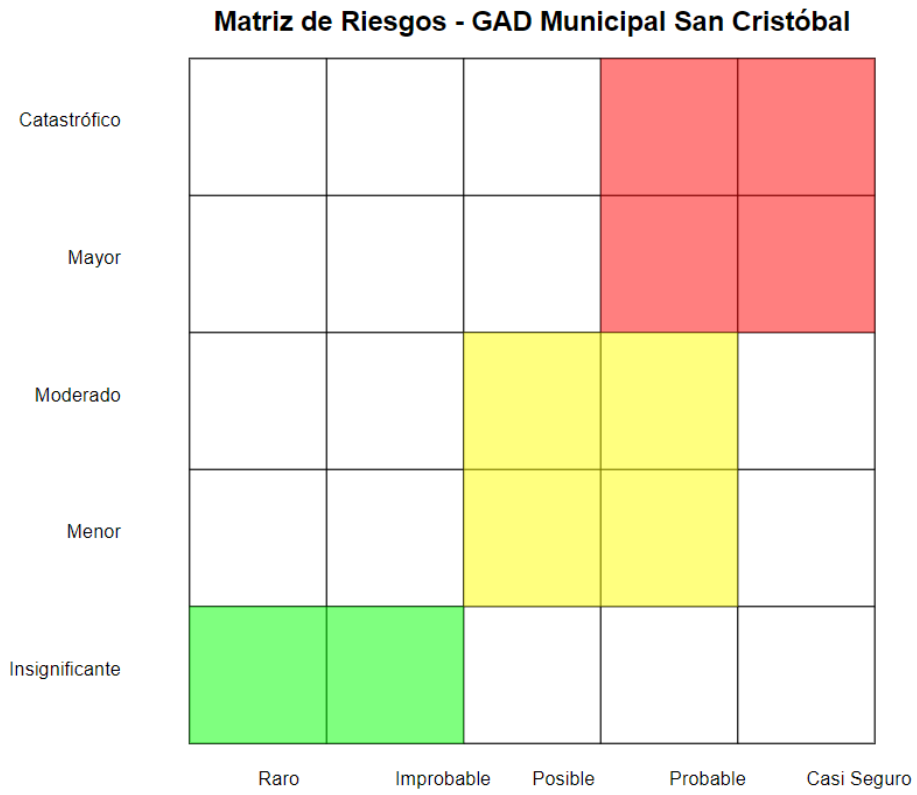
Ramírez, E., & González, P. (2023). Seguridad Perimetral Avanzada en Entornos Municipales. *Revista Iberoamericana de Sistemas, 12*(2), págs. 89-104.

Valencia, R., & Torres, M. (2024). Virtualization Security in Government Environments: Best Practices and Implementation Guidelines. *Government Information Quarterly, 41*(1), págs. 101-115.

ANEXOS

Se presenta la información consultada. Pueden ser, carta de compromiso, carta aval, instrumentos, evidencia fotográfica, entre otros que el autor considere necesario.

Anexo 1:



Anexo 2:

Formato de Encuesta

ENCUESTA DE EVALUACIÓN DE SEGURIDAD INFORMÁTICA GAD MUNICIPAL DE SAN CRISTÓBAL

Objetivo: Evaluar el nivel de conocimiento, prácticas y necesidades en materia de seguridad informática del personal del GAD Municipal de San Cristóbal.

Instrucciones:

- Lea cuidadosamente cada pregunta antes de responder
- Seleccione la opción que mejor represente su situación o conocimiento
- La información proporcionada es confidencial y será utilizada únicamente con fines de investigación

SECCIÓN A: INFORMACIÓN GENERAL

1. **Área o departamento al que pertenece:**

☐ Administrativo
☐ Financiero
☐ Técnico
☐ Operativo
Otros (especifique): _____

2. **Tiempo laborando en la institución:**

☐ Menos de 1 año
☐ 1-3 años
☐ 4-6 años
☐ Más de 6 años

3. **Nivel de acceso a sistemas informáticos:**

☐ Básico (solo email y ofimática)
☐ Intermedio (sistemas departamentales)
☐ Avanzado (sistemas críticos)
☐ Administrador de sistemas

SECCIÓN B: CONOCIMIENTOS DE SEGURIDAD

Utilizando la escala del 1 al 5, donde: 1 = Totalmente en desacuerdo 2 = En desacuerdo 3 = Neutral 4 = De acuerdo 5 = Totalmente de acuerdo

Políticas y Procedimientos:

1. Conozco las políticas de seguridad informática del GAD Municipal ☐**1** ☐**2** ☐**3** ☐ **4**☐ **5**

2. Entiendo los procedimientos para reportar incidentes de seguridad☐ **1**☐ **2**☐**3**☐**4** ☐**5**

3. Sé a quién contactar en caso de un problema de seguridad ☐**1**☐ **2**☐ **3**☐**4** ☐ **5**

Identificación de Amenazas:

1. Puedo identificar un intento de phishing ☐**1**☐ **2**☐ **3**☐**4** ☐ **5**

2. Reconozco cuando un sitio web no es seguro ☐ **1**☐**2** ☐**3**☐ **4**☐ **5**

3. Sé identificar software malicioso o sospechoso ☐ **1**☐ **2**☐ **3**☐ **4**☐ **5**

SECCIÓN C: PRÁCTICAS DE SEGURIDAD

10. ¿Con qué frecuencia cambia su contraseña?

☐ Nunca
☐ Solo cuando el sistema lo requiere
☐ Cada 3 meses
☐ Cada mes
☐ Otro (especifique): _____

11. ¿Qué método utiliza para recordar sus contraseñas?

☐ Las anoto en papel
☐ Las guardo en mi teléfono
☐ Uso un gestor de contraseñas
☐ Las memorizo
☐ Otro (especifique): _____

12. Cuando recibe un correo sospechoso, usted:

☐ Lo elimina inmediatamente
☐ Lo reporta al departamento de sistemas
☐ Consulta con compañeros
☐ Lo abre para verificar el contenido

Gestión de Información Sensible:

13. ¿Cómo maneja los documentos confidenciales?

☐ Los elimino después de usarlos
☐ Los archivos de forma segura
☐ Los comparto solo con personal autorizado
☐ No manejo documentos confidenciales

14. ¿Qué medios utiliza para compartir información laboral?

☐ Correo institucional
☐ WhatsApp
☐ Drives compartidos
☐ Dispositivos USB
☐ Otro (especifique): _____

SECCIÓN D: INCIDENTES Y RESPUESTAS

15. ¿Ha experimentado algún incidente de seguridad en los últimos 6 meses?

☐ Sí
☐ No
☐ No estoy seguro

16. Si respondió sí, ¿qué tipo de incidente?

☐ Virus/Malware
☐ Phishing
☐ Pérdida de datos
☐ Acceso no autorizado
☐ Otro (especifique): _____

17. ¿Cómo procedió ante el incidente?

☐ Lo reporté inmediatamente
☐ Intenté solucionarlo por mi cuenta
☐ Consulté con compañeros
☐ No hice nada

SECCIÓN E: NECESIDADES DE CAPACITACIÓN

18. ¿En qué áreas considera que necesita más capacitación? (Puede seleccionar múltiples opciones)

☐ Identificación de amenazas
☐ Gestión de contraseñas
☐ Protección de datos sensibles
☐
☐

Uso seguro de internet
Respuesta a incidentes
Otro (especifique): _____

19. ¿Qué modalidad de capacitación prefiere?

☐ Presencial
☐ Virtual
☐ Mixta
☐ Talleres prácticos

20. ¿Qué horario prefiere para las capacitaciones?

☐ Durante la jornada laboral
☐ Después de la jornada laboral
☐ Fines de semana
☐ Flexible/A demanda

SECCIÓN F: SUGERENCIAS Y COMENTARIOS

21. ¿Qué aspectos de la seguridad informática en el GAD Municipal considera que necesitan mejora? [Espacio para respuesta abierta]

22. ¿Qué sugerencias tiene para mejorar la seguridad informática en su área de trabajo? [Espacio para respuesta abierta]

23. ¿Qué obstáculos encuentra para implementar las prácticas de seguridad en su trabajo diario? [Espacio para respuesta abierta]

SECCIÓN G: VALIDACIÓN DE CONOCIMIENTOS PRÁCTICOS

24. En una escala del 1 al 5, ¿qué tan seguro se siente al:

a) Identificar correos de phishing? ☐**1** ☐**2** ☐**3** ☐**4** ☐**5**
b) Manejar información confidencial? ☐**1** ☐**2** ☐**3** ☐**4** ☐ **5**
c) Reportar incidentes de seguridad? ☐**1** ☐**2** ☐**3** ☐**4** ☐ **5**
d) Utilizar contraseñas seguras? ☐**1** ☐**2** ☐**3** ☐**4** ☐ **5**

25. ¿Qué haría en las siguientes situaciones?

a) Recibe un correo urgente de su supervisor solicitando sus credenciales: [Espacio para respuesta abierta]

b) Encuentra una unidad USB en su escritorio: [Espacio para respuesta abierta]

c) Un compañero le pide su contraseña para acceder a un sistema: [Espacio para respuesta abierta]

Firma del Encuestado: _____ Fecha: _____

Gracias por su colaboración en esta encuesta. Sus respuestas ayudarán a mejorar la seguridad informática del GAD Municipal.