DICTAMEN TÉCNICO.

Lugar y fecha: Asunción, 21 de julio del 2025
UOC Convocante: Servicio Nacional de Promoción Profesional (SNPP)
Unidad o área requirente: Dirección de Tecnología de la Información y comunicación
Funcionario o técnico responsable: Ing. Eder A. Añazco Greco
Dependencia y cargo que desempeña: Dirección de Tecnología de la Información y Comunicación.

Proyecto: *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) Y CENTRO DE OPERACIONES DE SEGURIDAD (SOC)*
Periodo: Anual

JUSTIFICACIÓN DEL PROYECTO:

La creciente sofisticación de ciberamenazas, como intrusiones, malware y accesos no autorizados, pone en riesgo la infraestructura tecnológica de la institución, que incluye redes corporativas, servidores y más de 1000 endpoints. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 y un Centro de Operaciones de Seguridad (SOC) con herramientas mixtas propietarias y de código abierto es técnicamente necesaria para detectar y mitigar problemas de seguridad en tiempo real, garantizando la ***confidencialidad, integridad y disponibilidad*** *de la información, y cumpliendo con los objetivos estratégicos de la institución.*

OBJETIVO GENERAL:

Fortalecer la capacidad de prevención, detección y minimización de intrusiones en la red de la institución.

OBJETIVOS ESPECÍFICOS:

- *Detectar mediante firmas o patrones de comportamiento intrusiones o intentos.*
- *Activamente establecer reglas de bloqueo en caso de detectar anomalías en la red.*
- *Responder de forma correcta incidentes de ciberseguridad.*
- *Mejora continua*

METAS Y ACTIVIDADES:

Metas	*Actividades*
Licitación para la adquisición de los equipos adjudicada	*- Elaboración de la documentación necesaria para la licitación* *- Aprobación del Dpto. Jurídico* *- Publicación* *- Apertura de sobres* *- Evaluación* *- Adjudicación*

Implementación SOC	*- Instalación, configuración y puesta en funcionamiento del SOC* *- Configuración de herramientas de remediación de vulnerabilidades.* *- Configuración de herramientas de código abierto.* *- Integración de feeds de inteligencia de amenazas (MISP, CERTpy, etc)* *- Pruebas de funcionamiento y escalabilidad*
Operación del SGSI	*- Implementación de 30 controles prioritarios basados en ISO/IEC 27001* *- Configuración de SIEM para monitoreo continuo y correlación de eventos* *- Desarrollo de playbooks para ransomware, phishing y DDoS* *- Auditorías iniciales (CIS, OWASP Top 10, etc)* *- Capacitación técnica de 300 horas para 10 técnicos* *- Sensibilización gamificada de 15 horas para 700 colaboradores*

RESULTADOS ESPERADOS:

- *Equipo de seguridad instalado, en funcionamiento y con detección de intrusiones configurada.*
- *Reducción del tiempo medio de detección (MTTD) a ≤60 minutos y del tiempo medio de respuesta (MTTR) en un 70% para el mes 7.*
- *Resolución de incidentes críticos en ≤24 horas.*
- *Infraestructura protegida con herramientas escalables de código abierto (Wazuh, TheHive, osTicket).*
- *Personal técnico capacitado y colaboradores sensibilizados, garantizando autonomía operativa.*

1. JUSTIFICACIÓN TÉCNICA

1.1. Protección de Infraestructura Crítica

La organización gestiona redes corporativas, servidores y más de 1000 endpoints, los cuales son vulnerables a amenazas como malware, explotación de vulnerabilidades y accesos no autorizados. Un SGSI basado en ISO/IEC 27001 permitirá establecer controles robustos para mitigar riesgos, mientras que el SOC, proporcionará monitoreo continuo y respuesta rápida a incidentes, reduciendo el tiempo medio de detección (MTTD) a ≤60 minutos y el tiempo medio de respuesta (MTTR) en un 70% para el mes 12.

2.2. Cumplimiento Normativo y del Pliego

El proyecto asegura la conformidad con el pliego de bases y condiciones, implementando políticas alineadas con ISO 27001, NIST CSF y CIS Controls. Las auditorías semestrales y la matriz de riesgos garantizarán el cumplimiento continuo.

2.3. Respuesta Efectiva a Incidentes

La formación en ciberseguridad con roles definidos (coordinador, analista, forense) y playbooks específicos para ransomware, phishing y DDoS permitirá una respuesta estructurada y eficiente. La integración de feeds de inteligencia de amenazas en el SOC mejorará la detección proactiva, mientras que simulaciones de incidentes fortalecerán la preparación del equipo.

2.4. Escalabilidad y Sostenibilidad

El uso de herramientas de código abierto asegura escalabilidad sin costos recurrentes de licenciamiento. Estas herramientas, combinadas con herramientas propietarias garantizan la continuidad del servicio durante los 24 meses del proyecto y más allá.

2.5. Fortalecimiento de Capacidades

La capacitación técnica de 300 horas para 2 técnicos en herramientas y análisis de vulnerabilidades, junto con la sensibilización gamificada, asegura la transferencia de conocimiento y la adopción de una cultura de ciberseguridad.

2.6. Reducción de Riesgos Operativos

El diagnóstico inicial con auditorías CIS, OWASP Top 10 identificará vulnerabilidades críticas, permitiendo priorizar su mitigación. La optimización de reglas de detección reducirá falsos positivos, mejorando la eficiencia del SOC. Además, la garantía de 24 meses y el soporte post-implementación aseguran la estabilidad operativa.

3. BENEFICIOS ESPERADOS

- ***Seguridad Reforzada**: Protección de la confidencialidad, integridad y disponibilidad de la información en redes y endpoints.*
- ***Cumplimiento Normativo**: Alineación con ISO 27001 y el pliego de bases, con auditorías que validan el cumplimiento.*
- ***Respuesta Ágil**: Reducción de MTTD y MTTR, con resolución de incidentes críticos en ≤24 horas.*
- ***Sostenibilidad**: Uso de herramientas de código abierto para minimizar costos a largo plazo.*
- ***Capacitación Efectiva**: Equipo interno capacitado y colaboradores sensibilizados, reduciendo errores humanos.*
- ***Autonomía**: Transferencia de conocimiento completa para la operación independiente del SOC y SGSI.*

4. CONCLUSIÓN

La implementación de un SGSI y un SOC es técnicamente viable y necesaria para mitigar riesgos de ciberseguridad, cumplir con requisitos normativos y garantizar la continuidad operativa. La combinación de herramientas de código abierto, capacitación intensiva y auditorías periódicas asegura una solución escalable, sostenible y alineada con los objetivos estratégico-operativos de la organización.

Firma del técnico o responsable del área requirente:

Aclaración: *Ing. Eder Añazco G.*
Director
Dirección de TIC - SNPP

Firma del responsable UOC:

Aclaración: