



TEMPORU MARANDU
HA ÑEMOASÁIRA
Moreno decha
Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

 TETÃ REKUÁI
 GOBIERNO NACIONAL

*Paraguay
de la gente*

CONSULTA PÚBLICA PROYECTO SECURITY OPERATION CENTER MITIC

PROGRAMA DE APOYO A LA AGENDA DIGITAL

ASUNCIÓN, PARAGUAY

2021



CONTENIDO

1. Antecedentes y Situación actual	1
2. Descripción del Proyecto	2
Principales servicios considerados que prestará el SOC:	2
Concepto Organizacional componentes del SOC y resultados producidos:	3
Componentes del Proyecto SOC:	3
Arquitectura tecnológica del Proyecto:	4
Infraestructura edilicia y equipamiento físico:	5
Conectividad e interconexión:	6
3. Condicionantes previas / pre-existentes	7
4. Características deseables	8
5. Mecánica de la Consulta	9
6. Información de Contacto	10



1. Antecedentes y Situación actual

Una de las principales atribuciones del MITIC, en su rol de autoridad de ciberseguridad, es la gestión de incidentes cibernéticos de seguridad en todo el ecosistema digital nacional. Igualmente, una atribución es diseñar y ejecutar estrategias, iniciativas y proyectos de protección de los sistemas y redes gubernamentales.

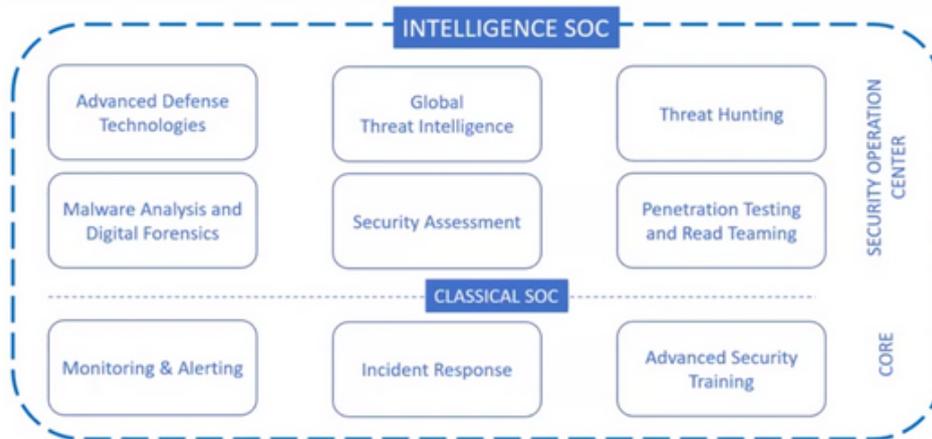
Actualmente la gran mayoría de las instituciones públicas no cuentan con un mecanismo adecuado de detección eficiente que permita obtener visibilidad de eventos, ni cuantificar el grado de amenazas al que están expuestas. Hoy en día sabemos que un ciberataque, especialmente, aquellos más graves, consta de una serie de acciones maliciosas que van desde una intrusión inicial, escalación de privilegios, robo de credenciales, movimientos laterales, hasta conseguir los objetivos de los adversarios. Esas acciones muchas veces pasan desapercibidas, a veces durante muchos meses, y el ciberataque recién es detectado cuando se manifiestan sus consecuencias. En muchos casos, éstas consecuencias ni siquiera son visibles (ejemplo: robo de información estratégica), por lo que el ciberataque no es detectado nunca.

En el MITIC opera el Centro de Respuestas a Incidentes Cibernéticos (CERT-PY), el punto focal de coordinación y respuesta a incidentes que ocurren en el ecosistema digital. El CERT-PY cuenta con analistas y herramientas necesarias para gestionar, responder y coordinar los incidentes que le son reportados. Los incidentes de seguridad (amenaza materializada) son reportados al CERT-PY a través de un sistema de gestión de ticketing, donde los analistas clasifican de acuerdo a su criticidad, los investigan y remiten recomendaciones a los afectados para contenerlos, mitigarlos y erradicarlos.

Sin embargo, el CERT-PY necesita tomar conocimiento del incidente para poder actuar, ya sea a través del reporte por parte de una persona o mediante datos de fuentes abiertas; el CERT-PY no administra, mantiene, gestiona ni tiene acceso a las redes equipos o sistemas de otras instituciones, y por tanto, no cuenta con visibilidad sobre los eventos o indicios de compromiso que pudiera encontrarse en esas redes o sistemas.

Si bien, de acuerdo a la Resolución MITIC N° 346/2020 existe una obligatoriedad de que todo incidente debe ser reportado al CERT-PY por parte de los Responsables de Seguridad de la Información (RSI) de Gobierno, la gran mayoría de los incidentes no son detectados ni percibidos visiblemente, por lo que el RSI no puede reportarlo porque no se llega a enterar del incidente hasta después de materializada la amenaza.

Por tal motivo se requiere de un mecanismo que permita a través de diversos medios, servicios, procesos, tecnologías, herramientas y personas obtener **visibilidad de eventos**, elevar las capacidades de prevención, detección y respuesta, así como establecer los mecanismos más eficiente para minimizar y evitar eventos disruptivos que acaban afectando a los servicios que se prestan para el ciudadano. La expectativa con el proyecto es adoptar un enfoque **Proactivo** vs el modelo **Reactivo** clásico que limitaba la actuación del CERT-PY solo a cuando se materializaba una amenaza y por ende se generaba un incidente.



El proyecto de Centro de Operaciones de Seguridad (SOC) sería este complemento necesario que estaría dotando al CERT-PY con capacidades proactivas, garantizando además, que las distintas amenazas que hoy están desafiando los mecanismos de seguridad defensiva en las OEE sean contenidas/erradicadas antes de escalar a un incidente.

2. Descripción del Proyecto

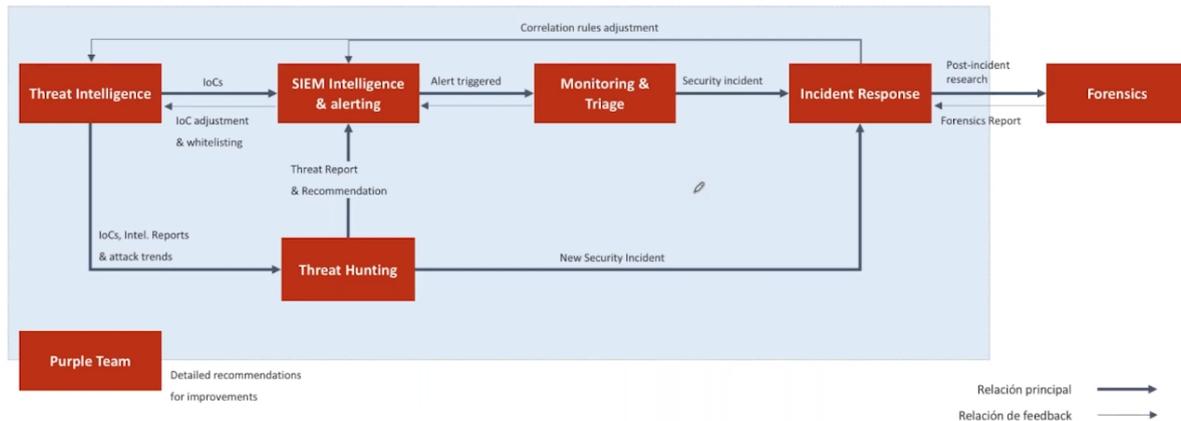
En el marco del Préstamo del Banco Interamericano de Desarrollo (BID), PR - L1153. Programa de Apoyo a la Agenda Digital, el MITIC financiará el proceso de diseño, construcción, despliegue, calibración y mantenimiento inicial de un Security Operation Center Gubernamental (govSOC), junto con su operación, durante el tiempo de duración de dicho programa (hasta Mayo 2025).

El MITIC busca adoptar un modelo de seguridad **MDR (Managed Detection and Response)**, convirtiéndose en un proveedor de servicios SOC para el Estado, que permite pasar de una posición reactiva clásica a una posición proactiva, logrando con esto no solo ganar visibilidad centralizada sino además poder adelantarse a la materialización de las amenazas que impactan negativamente la continuidad de servicios institucionales. Como expectativa final buscamos la mejora constante hacia modelos avanzados de ciberseguridad, como la ciberdefensa proactiva e impulsada por inteligencia artificial, machine learning, deep learning, etc.

Principales servicios considerados que prestará el SOC:

- Monitoreo de eventos a través de diversas fuentes de información.
- Análisis y detección de amenazas, vulnerabilidades y alertas de ciberseguridad
- Aportar contexto en el manejo de la respuesta a incidentes de seguridad cibernética
- Concienciación de la situación de ciberseguridad institucional e informes
- Detección de amenazas y desviaciones de líneas bases de ciberseguridad que pudieran generar un incidente.
- Intercambio de información de seguridad e inteligencia de amenazas (modelo ISAC)

Concepto Organizacional componentes del SOC y resultados producidos:



Es fundamental que dicho proyecto no sólo se ajuste a las necesidades actuales, sino que cuente con la capacidad de crecimiento ordenado, seguro, escalable y sostenible por un período importante de tiempo basado en las siguientes expectativas:

1. Que sea sostenible en el tiempo tanto técnica como económicamente y ajustable al Plan de ejecución Presupuestaria del MITIC
2. Que se alinee a los modelos de madurez del SOC (SOC-CMM) con el CERT-PY (SIM3) para asegurar la calidad y continuidad en las Operaciones Cibernéticas.
3. Que se integre perfectamente al flujo de trabajo del CERT-PY, ampliando el espectro de sus servicios.

Componentes del Proyecto SOC:

Un Security Operation Center (SOC) está conformado por 3 elementos; personas, procesos y tecnología. Las personas en el SOC tienen roles y responsabilidades definidos, ellos aprovechan las capacidades de la tecnología (**HERRAMIENTAS, INFRAESTRUCTURA, etc**) para ejecutar procesos que por un lado (**INPUT**) que analizan, procesan, correlacionan volúmenes de eventos para entregar servicios de ciberseguridad (**OUTPUT**) que permitan mitigar, detectar y responder a los incidentes.

Los elementos mínimos a considerar como parte del proyecto SOC son los siguientes:

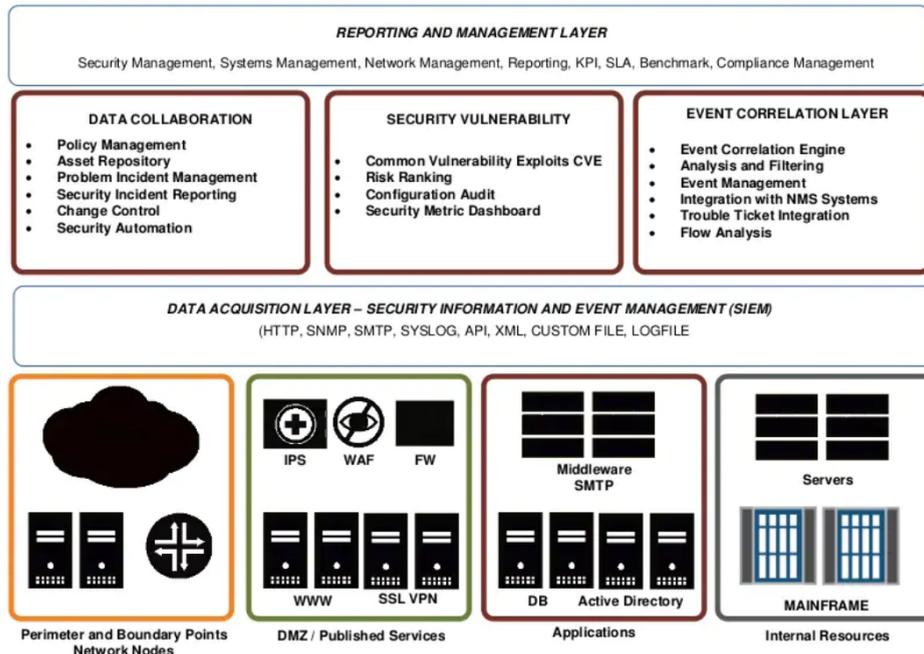
1. **Capa de Adquisición:** todos aquellos elementos (herramientas, software, servicios, plataformas, feeds, etc) que permitan obtener eventos relevantes de las organizaciones clientes, tanto desde sus propios sistemas y redes, así como también de fuentes abiertas, enriquecidas con información de inteligencia.
 - a. Log Management & Collection, OSQuery, Traffic Capture, Flow Capture, EDR.
 - b. Plataformas o servicios de Threat Intelligence
2. **Capa de Reporte y Administración:** todos aquellos elementos que permitan visualizar, correlacionar, integrar, analizar, enriquecer, responder, gestionar, priorizar y actuar ante los eventos correlacionados que han sido capturados por los elementos de la capa de adquisición.



- a. SOC Metrics, SIEM, SOAR, Incident Management Case, DFIR Vaults, Rapid Response Solutions.
 - b. Soluciones o servicios de Breach & Attack Simulation/Emulation, Soluciones o servicios de Security Assessment y Penetration Testing automatizado
 - c. Herramientas o servicios de Malware Analysis & Digital Forensic, Servicio o Soluciones de Threat Hunting,
3. **Capa de Hardware y conectividad:** todos aquellos elementos de infraestructura física que fueran requeridos (en caso de que la solución propuesta sea On-Premise) para soportar el software, tanto de core y/o de los colectores, sensores, agentes u otros elementos
- a. Infraestructura de core: Servidores, Entornos de Virtualización, Appliance, Switch, UTM, Solución para videowall 3x3
 - b. Conectividad dedicada para la red de operaciones del SOC y la infraestructura del core y sistema telefonía IP
 - c. Sistemas de protección, seguridad y redundancia de la infraestructura del core del SOC: Log Forensic Retention Server, AntiDDoS, WAF, controles de acceso físico a Rack, ..
4. **Formación/Capacitación continua** para Miembros del SOC/CERT-PY : Cursos, certificaciones, planes y plataformas automatizadas de aprendizaje, plataformas de cyberdrills, etc, que cubran los siguientes campos:
- a. Incident Handling & Response Career Path
 - b. Incident Management Career Path
 - c. Digital Forensic Career Path
 - d. Executive Management Career Path
 - e. Especializaciones (DevSecOps, SOC Career Path, Threat Intelligence)

Arquitectura tecnológica del Proyecto:

La siguiente imagen describe de modo general la arquitectura lógica del SOC a considerar. No consideramos la capa de hardware en esta imagen para no limitar los distintos modelos de soluciones SOC que pudieran ofrecer, pero para efectos del proyecto se considera implícita en caso de que se aplique lo anterior al escenario y soluciones propuestas.



La arquitectura del SOC consumirá eventos de un dispositivo colector de eventos o sonda (sensor y/o agente) que deberán ser desplegados en la infraestructura de la institución cliente, que a su vez consumirá, analizará y correlacionará los eventos producidas en éstas y reportará alertas (eventos correlacionados) al core del SOC del MITIC. Los orígenes de eventos para esos colectores, podrían ser netflow, packet capture, logs.

Para ello, dos posibles escenarios de despliegue serían:

- Modelo Distribuido: los eventos se capturan en la institución cliente, se normalizan pero se correlacionan en el core del SOC
- Modelo Federado: el core del SOC recibirá únicamente alertas, las cuales fueron correlacionadas previamente en la institución cliente

Se debe tener en cuenta que también se desea ganar visibilidad sobre la propia infraestructura de servicios del MITIC (shared webhosting basado en CPanel/WHM y servicios de cloud basados en contenedores).

Infraestructura edilicia y equipamiento físico:

El SOC está planificado y diseñado, a priori, para ocupar un espacio físico en las instalaciones del nuevo DataCenter y NOC de Servicios del MITIC, en una superficie de 50 mts cuadrados para oficinas de operaciones. Está pensado para alojar 7 analistas, 1 SOC Manager y 2 Ingenieros de Seguridad.

La construcción edilicia de dicho espacio, así como el equipamiento básico del espacio de oficinas (mobiliario, PC/notebook, pantallas y periféricos) están contemplados dentro del proyecto de Construcción de Datacenter de Gobierno, por lo tanto escapa al alcance del proyecto SOC.

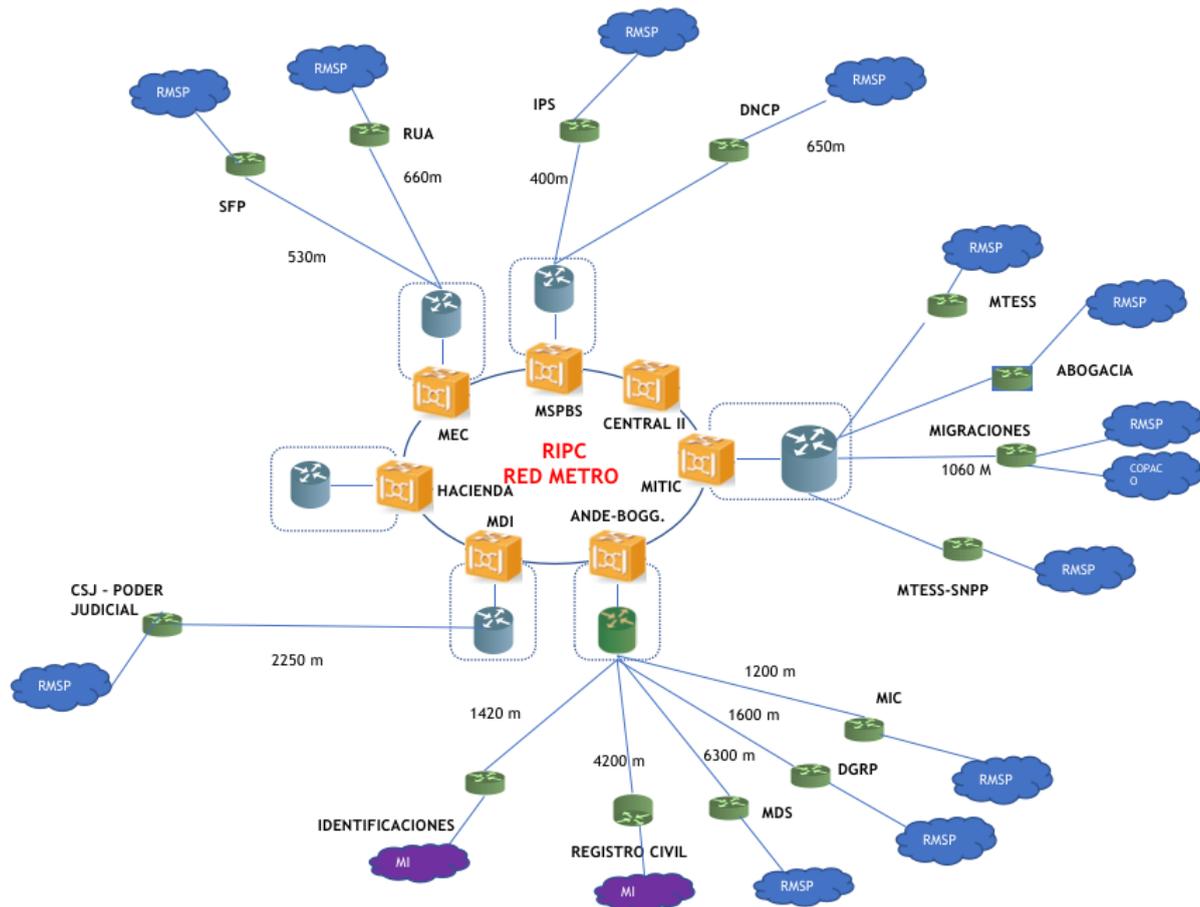


Igualmente, el Datacenter proveerá al SOC un servicio en modalidad de Colocación (Collocation), disponiendo 2 racks genéricos de 42 U. Cualquier otro requerimiento de infraestructura y seguridad física específica de un SOC deberá ser contemplado en este proyecto.

Conectividad e interconexión:

La conectividad que permita enviar el flujo de información de las instituciones clientes hasta el core del SOC forma parte del proyecto y deberá ser contemplado tanto técnica como financieramente, tanto para la implementación como para la sostenibilidad del proyecto.

Actualmente, se cuenta con una Red Nacional de fibra óptica que interconecta varias instituciones públicas, de acuerdo al siguiente diagrama:



RMSP: Red Metropolitana del Sector Públicos
MI: Ministerio del Interior.

Para la interconexión con cualquier otra institución deberá contemplarse algún mecanismo de conectividad a través de VPN.



El SOC deberá contar con su propia conectividad de salida Internet, independiente de los servicios que se encuentren en el Datacenter de Gobierno. Se estima una conectividad de al menos 200 Mbps redundante con bloques IPv4 públicos /29.

3. Condicionantes previas / pre-existent

- Todas las soluciones propuestas deben considerar que el backend debe ser operado por los analistas del SOC/CERT-PY.
- Los escenarios tecnológicos de las instituciones son heterogéneos; incluso, muchas de ellas no cuentan con mecanismos de gestión centralizada de sus activos (controladora de dominio, por ej).
- El servicio de SOC será un servicio que el MITIC ofrecerá a demanda y, a priori, de manera gratuita, a instituciones públicas. No se pretende, a priori, establecer la obligatoriedad del uso de dicho servicio por parte de los OEE.
- El CERT-PY no administra ni configura equipos en las OEE.
- Las OEE muchas veces no cuentan con personal suficiente ni con personal técnico calificado, en algunos casos incluso no hay personal de TIC.
- Las OEE manejan sus propias planificaciones de ejecución presupuestaria.
- De acuerdo a la proyección actual, el límite de fecha para la ejecución presupuestaria de este proyecto es diciembre de 2024.
- No se conoce de antemano la cantidad de instituciones que solicitarán y/o aceptarán el servicio de SOC del MITIC ni el ratio de crecimiento de éstas. Se estima que, en una primera fase (primeros 6 meses) podría haber alrededor de 5 instituciones clientes. Actualmente existen 70 Instituciones públicas que cuentan con un Responsable de Seguridad de la Información, (Cybersecurity Point of Contact) siendo todas estas potenciales instituciones clientes.
- No se conoce con exactitud ni se tiene control sobre la cantidad de activos de cada potencial institución cliente.
- El arranque del proyecto no puede estar condicionado a la fecha de finalización de la edificación y puesta en funcionamiento del Datacenter del MITIC, debiendo preverse que, en una primera etapa, los sistemas puedan estar alojados temporalmente en infraestructura existente del MITIC u otro proveedor, hasta su instalación definitiva en el Datacenter.



4. Características deseables

Para el proyecto se evaluarán todas aquellas soluciones que permitan la creación de un Centro de Operaciones de Ciberseguridad gubernamental con alcance nacional. Estas soluciones pueden proponerse para ser implementadas de forma In-House, con deployments tanto On-Premise como SaaS/IaaS/PaaS, siendo el backend operativo y el triage, análisis, investigación y demás operaciones gestionadas por los analistas del SOC/CERT-PY.

- Sostenibilidad económica: Esperamos que las propuestas sean sostenibles económicamente, minimizando los costos de mantenimiento y operación.
- Escalabilidad: Se valorará que las propuestas sean económica y técnicamente escalables, considerando que en un futuro pudiera haber más de 100 instituciones clientes potenciales. Se preferirá aquellas propuestas que impliquen un mínimo de esfuerzo y recursos a la hora de la incorporación de un nuevo cliente.
- Interoperabilidad y neutralidad tecnológica: se valorará aquellas soluciones o propuestas que no estén condicionadas a una única tecnología o marca en particular, pudiendo ser interoperables, compatibles o reemplazables con distintas tecnologías o marcas, es decir que sean **agnósticas**.
- Sostenibilidad técnica: Se valorará aquellas propuestas basadas en herramientas estándar, de código abierto, conocidos por la industria y comunidad y de licenciamiento gratuito y/o de bajo costo, que permitan no solo la sostenibilidad económica del proyecto, sino también maximizar la inversión en servicios profesionales de implementación y/o mantenimiento. Además, esto permitirá que las soluciones puedan ser mantenidas en un futuro por otras empresas de tecnología (nacionales o internacionales), la comunidad y/o personal de MITIC.
- Maximización de alcance: Se valorará aquellas propuestas que, comparado a otra de igual presupuesto, permita maximizar el alcance de los servicios (mayor cantidad de clientes potenciales, mayor nivel de visibilidad, mayor nivel de granularidad, mayor grado de actuación, mayor tiempo de servicio, etc.)
- Mínimo esfuerzo/costo del cliente: se valorará aquellas propuestas que, para la integración de un nuevo cliente, requiera un mínimo esfuerzo, tiempo, conocimiento, adecuación tecnológica y recursos económicos de parte del cliente. En las propuestas presentadas deben aclararse las condiciones y supuestos que deben darse por parte de la institución cliente.
- Movilidad / BYOD: se valorará aquellos despliegues que permitan la continuidad en la correlación de eventos aún en una organización con una política de movilidad o Bring-your-own-Device (BYOD)
- Multi-tenant: se valorará aquellas propuestas que permitan un ambiente multi-institución, que separe los dominios y contextos de seguridad pero que a la vez nos permita interactuar en modalidad Rapid Response con los ambientes. Se valorará aquellas soluciones que permitan que cada institución cliente tenga visibilidad, e incluso capacidad de acción (cambios de reglas y configuraciones y acciones de respuesta) sobre el dominio y contexto que le corresponde.
- Maximización de automatización: considerando la limitación del MITIC para aumentar y/o mantener el staff de analistas técnicos, se valorará aquellas propuestas que minimicen el



esfuerzo humano, maximicen la automatización y cuya escalabilidad no dependa (o dependa lo menos posible) del aumento de analistas.

- Modelo de costos flexibles: En el caso de servicios por suscripción, serán preferidas aquellas propuestas en un modelo Pay-as-you Grow y/o de pago adelantado (compra de "créditos de uso"), considerando la incertidumbre de crecimiento y el tiempo límite de la posible ejecución presupuestaria del proyecto

5. Mecánica de la Consulta

La presente consulta pública está dirigida a los posibles interesados en presentar herramientas, soluciones y/o servicios que puedan ser considerados para la implementación del SOC de acuerdo con el apartado 2 anterior.

- Aquellos interesados en participar en esta consulta pública deberán enviar sus propuestas, incluyendo información de las soluciones o servicios que proponen, características, descripciones, costos aproximados, las consideraciones técnicas y de cualquier otro tipo de información que pueda ser relevante para el diseño del proyecto.
- Se aceptarán propuestas de soluciones completas en un modelo "llave en mano", así como también de soluciones o servicios parciales que solo cubran alguna de las partes del proyecto.
- Se aceptarán todo tipo de propuestas que cubran los distintos componentes del SOC en sus capas principales, así como los distintos tipos de implementación (In-House, Outsourced). Pudieran ser basadas en soluciones comerciales, de código abierto, respaldadas por un vendor, respaldadas por un equipo o empresa de desarrollo de software en modalidades software factory, desarrolladas a medida ("from scratch") etc., buscando garantizar la sostenibilidad y transferencia de conocimiento, para operar y mantener la solución al término de los 3 años de acompañamiento y soporte en la operación y el mantenimiento.
- La fecha límite para la recepción de propuestas es el día **29 de octubre del corriente año**, vía correo electrónico a la dirección audiencias_ciber@mitic.gov.py.
- No se atenderán aquellas propuestas e informaciones que no se encuentren directamente relacionadas con el objeto de la presente consulta.
- Esta consulta pública no tiene carácter vinculante para el Ministerio de Tecnologías de la Información y Comunicación (MITIC) ni para la Dirección Nacional de Contrataciones Pública (DNCP), pero la información recabada será de suma importancia para su utilización, tanto para establecer criterios y tomar decisiones en cuanto al modelo de solución, arquitectura, herramientas y servicios asociados, así como también para estimación de costos e informaciones referenciales en el llamado correspondiente.



6. Información de Contacto

- Ing. Gabriela Ratti; Dirección General de Ciberseguridad y Protección de la Información
Correo: gratti@mitic.gov.py - Tel.: +595 21 2179000
- Ing. Ruslan Osorio; Responsable de Proyecto SOC
Correo: rosorio@mitic.gov.py - Tel.: +595 21 2179000