Programa de Ciberseguridad para Infraestruct. Críticas de Información (ICI)

Diseño de alto nivel para G-SOC de Gobierno de Argentina

Referencia del Proyecto

OP22-0472

Versión: 1.2

Estado: Aprobado
Fecha: 08/07/2022

Autores
Equipo de CSA

Cliente

BANCO INTERAMERICANO DE DESARROLLO

TLP: RED

Este documento contiene información confidencial que no se puede compartir con terceros, más allá de los responsables del Proyecto del BID y la Jefatura de Ministros del Gobierno de Argentina.

Plaza de Santo Domingo de Guzmán, 1. Pl. 6ª - 09004 Burgos
Paseo de la Castellana, 93, Pl. 12ª - 28046 Madrid
Torre Expomurcia. Avda. Miguel de Cervantes 45, Planta 4, oficina B - 30009 Murcia
C/ Prolongación Ramón y Cajal, 5 Edif. Orquídea, portal 2, Pl. 2 ª, Of. 8- 38003 S/C de Tenerife

© 1996-2022 CSA. Todos los derechos reservados. Estrictamente confidencial. La presente información está dirigida a los destinatarios y únicamente puede ser utilizada a los efectos que se indican en la portada del documento. Si el receptor no es la persona a la que va dirigida esta comunicación confidencial, se le notifica que la distribución o copia de esta comunicación está terminantemente prohibida.

Registro de cambios

Versión	Fecha	Revisado	Resumen de los cambios producidos
0.1	28/06/2022	Equipo de CSA	Borrador de la primera versión
0.2	04/07/2022	Equipo de CSA	Borrador completo de la primera versión
1.2	08/07/2022	Equipo de CSA	Aprobado

Índice

1. Introducción 4

2. Capacidades Nacionales 5

3. Servicios de la Capacidad de Detección 7

3.1. Detección de Activos 7

3.1.1. Detección e Identificación de Activos Tecnológicos y Humanos 7

3.1.2. Identificación y Protección de Infraestructuras Críticas de Información 8

3.2. Detección de Amenazas 8

3.2.1. Programa Nacional de Sondas 9

3.2.2. Cibervigilancia Preventiva 10

3.2.3. Plataforma de Agregación de Eventos 10

3.2.3.1. Diseño y puesta en marcha de la Plataforma de Agregación de Eventos 11

3.2.3.2. Adquisición de la Plataforma de Agregación de Eventos 11

3.2.3.3. Despliegue, operación y soporte de la infraestructura tecnológica de la Plataforma de Agregación de Eventos 11

3.2.4. Plataforma de Big Data 12

3.2.5. Implantación de SOAR 13

3.2.6. Seguridad Ofensiva (Red Team) 13

3.2.7. Análisis de Vulnerabilidades 14

4. Servicios de la Capacidad de Coordinación 15

4.1. SIEM 16

4.1.1. Adquisición de la infraestructura tecnológica SIEM para el CERT / G-SOC 16

4.1.2. Operación L1-L2 sobre el SIEM del CERT / G-SOC 17

4.2. Plataforma Nacional de Notificación y Coordinación de Incidentes 18

4.3. Plataforma Nacional de Intercambio de Información de Amenazas 19

4.4. Consultoría de Análisis de Riesgos 20

4.5. Consultoría de Comunicación 21

5. Servicios de la Capacidad de Respuesta 22

5.1. Defensa Activa 22

5.2. IRT (Incident Response Team) 23

5.3. Threat Hunting 23

5.4. Mitigación de Denegación de Servicio Distribuida 24

5.5. Detección de Fuga de Información 24

1. Introducción

En este documento se describe a alto nivel el diseño que se ha concebido para el G-SOC o Governmental Security Operations Center (SOC Gubernamental) de Gobierno de Argentina.

En primer lugar, se describen las capacidades que se pretenden adquirir con este G-SOC. Dichas capacidades se articulan en varios sub-elementos y estos a su vez se materializan en servicios, desarrollados a lo largo de esta memoria.

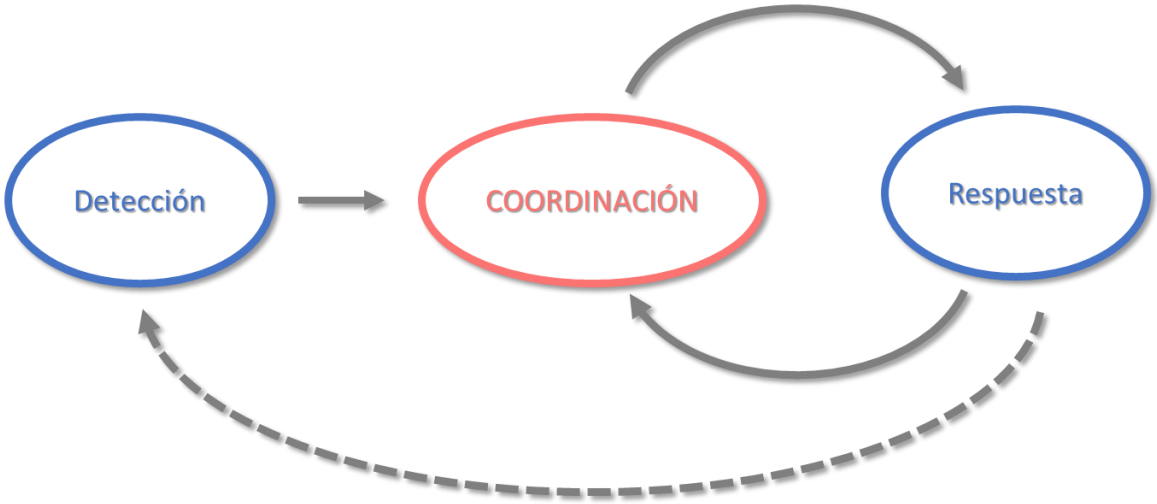
Este documento ofrece un dimensionamiento estimado de los grandes componentes del G-SOC.

Con la ejecución de este proyecto se espera dotar a Gobierno de Argentina de una infraestructura y una capacidad de operación óptimas para hacer frente a los retos en ciberseguridad que se presentan en el mundo actual.

2. Capacidades Nacionales

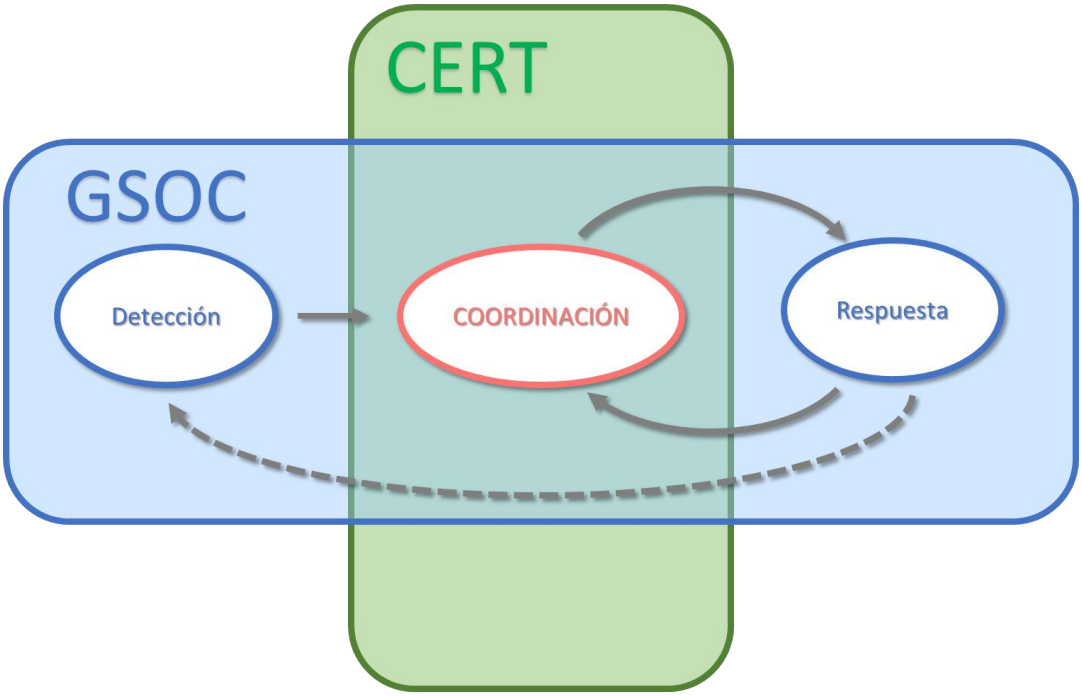
Entendemos que la aportación fundamental de un SOC Gubernamental consiste en el despliegue de una serie de capacidades. Estas capacidades se implementarán mediante servicios, productos, herramientas, etc., pero estos ítems son solo medios a través de los cuales se hacen efectivas estas capacidades.

En el siguiente diagrama se representan las tres Capacidades Nacionales que implementa este G-SOC, así como sus conexiones y realimentaciones:



1. **Detección**. Es la capacidad por la que empieza todo, ya que necesitamos tener claro qué tenemos y qué está pasando en nuestros activos. Por ello, será el área que se despliegue en primer lugar y donde haya una inversión inicial más fuerte.

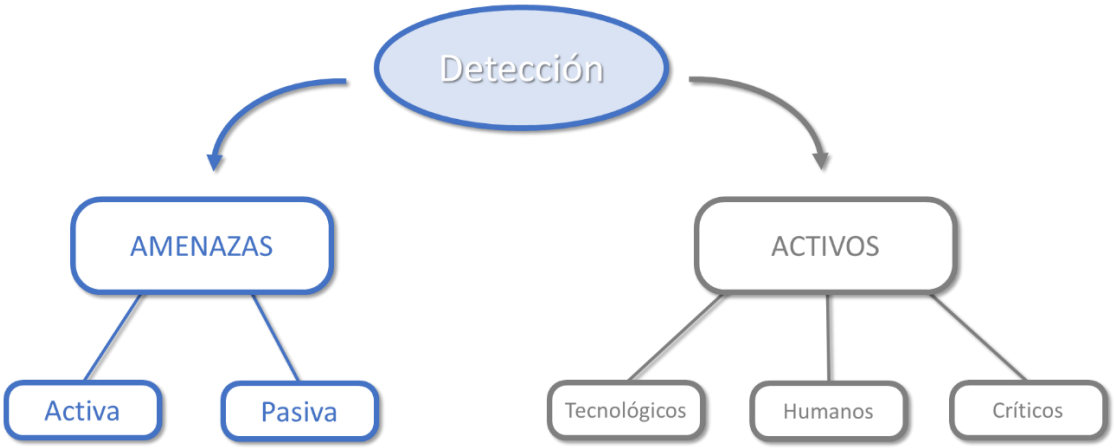
2. **Coordinación**. En la capacidad de coordinación se haya el verdadero centro de operaciones del SOC gubernamental, ya que allí se analizan los eventos y se tratan los incidentes, tanto en el aspecto técnico como en el comunicativo.
   La capacidad de coordinación será un componente común entre el G-SOC y el CERT ya existente. La estructura actual del CERT accederá a dicha capacidad, de forma que existirá una única capacidad de coordinación común.



3. **Respuesta**. Ante los incidentes confirmados es necesario disponer de una serie de equipos y servicios que den respuesta a los mismos, logrando mitigar el impacto y aplicando las correcciones o aprendizajes extraídos de un incidente de seguridad.
   La capacidad de respuesta realimentará a la de coordinación con los avances que obtengan, manteniendo una sincronización fluida entre las capacidades de coordinación y de respuesta. De igual forma, las investigaciones efectuadas en la capacidad de respuesta enviarán información a la capacidad de detección, con el fin de mejorar su alcance.

3. Servicios de la Capacidad de Detección

Dentro del concepto de detección, en esta arquitectura se plantean dos familias de detecciones: detecciones de activos y detecciones de amenazas.



3.1. Detección de Activos

En la parte de detección de activos, lo que se quiere obtener es el conocimiento de qué tenemos (activos tecnológicos), quién gobierna lo que tenemos (activos humanos) y dar un tratamiento especial a los activos críticos, que en cualquier SOC se deben tratar a velocidad diferente del resto de activos.

3.1.1. Detección e Identificación de Activos Tecnológicos y Humanos

Los activos se definen como: *cualquier recurso de la organización necesario para desempeñar sus actividades diarias y cuya indisponibilidad o deterioro genera un agravio o coste*[1], es por ello que como fase principal de la capacidad de detección encontramos el servicio de identificación de activos tecnológicos y humanos, pues la identificación y valoración de los activos es indispensable para poder definir correctamente la magnitud del riesgo y aplicar en consecuencia el nivel de protección necesario a cada uno de estos activos.

Cada uno de los activos presenta unas características concretas, lo que genera que no todos requieran el mismo nivel de protección y/o monitorización, bien sea por el tipo de información que contienen, por su estado de conservación o por la criticidad que su disponibilidad supone para el desarrollo de los procedimientos y servicios diarios de la organización.

De igual manera, junto a la identificación de activos tecnológicos, es necesario documentar y validar la responsabilidad del personal que tiene acceso a los mismos, sus roles y responsabilidades dentro de la organización, lo que permitirá garantizar las propiedades de disponibilidad (accesible en todo momento

[1] Gestión de riesgos: una guía de aproximación para el empresario, INCIBE: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

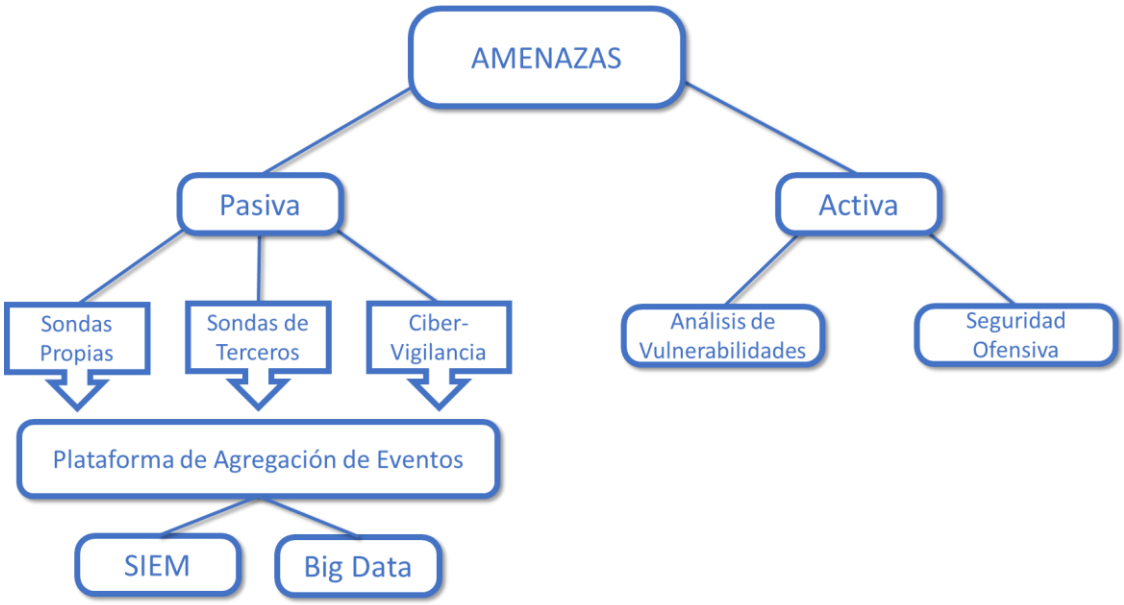
con autorización), integridad (exactitud en la información), confidencialidad (restricción especifica), autenticidad (sin alteración) y trazabilidad (registro de acceso y gestión) de la información de la empresa[2].

3.1.2. Identificación y Protección de Infraestructuras Críticas de Información

En el año dos, se ha planificado una partida para la identificación de ICIs (Infraestructuras Críticas de Información) y otra para el diseño de los planes de protección de las ICIs identificadas. Estos ítems pertenecen al IP 1: "Marco institucional y normativo para la identificación y protección de ICI aprobado". Aunque estas partidas quedan un poco más alejadas del conjunto de servicios que se recogen en este documento anexo sobre el diseño del G-SOC, la identificación y protección de ICIs igualmente debe formar parte de la Capacidad de Detección que aquí se explica. De hecho, como su propio nombre indica, estos activos deben tratarse de una forma particularmente cuidadosa por su criticidad, así como por la normativa especial que les aplica.

3.2. Detección de Amenazas

Aparte de saber qué activos tenemos, necesitamos identificar cuáles son las amenazas presentes en estos activos tecnológicos. Para ello, contaremos con métodos pasivos de recolección de información, mediante el Programa Nacional de Sondas y la Cibervigilancia Preventiva, y métodos activos de análisis de vulnerabilidades y red-teaming.



[2] "IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN, RIESGOS Y CONTROLES ASOCIADOS PARA LA EMPRESA ESTRATEGIAS EMPRESARIALES DE COLOMBIA BAJO LA NORMA ISO 27001 E ISO 31000", Borrero Ochoa (UNAD Colombia) https://repository.unad.edu.co/bitstream/handle/10596/35641/pcborreroo.pdf

3.2.1. Programa Nacional de Sondas

Para desarrollar e implementar la capacidad de detección de amenazas pasiva, es necesario disponer de visibilidad en el tráfico que circula por las redes de los organismos a proteger. Con dicho objetivo, se desarrollará un programa homólogo al Sistema de Alerta Temprana que el CCN-CERT comenzó a desplegar en España en el año 2008[3], cuyo fin es la detección en tiempo real de las amenazas e incidentes que afecten al organismo adscrito, con la intención de reducir su impacto y alcance.

Mediante el análisis del tráfico intercambiado entre la red interna del organismo e Internet, se consiguen detectar patrones de distintos tipos de ataque y amenazas, evitando su expansión y respondiendo de forma rápida ante el incidente detectado. Esta visibilidad también posibilita generar normas de actuación que eviten futuros incidentes. Además, gracias al almacenamiento de eventos a lo largo del tiempo, es posible contar con una panorámica completa y veraz de la situación de los sistemas adscritos al Programa Nacional de Sondas argentino, que permite una acción preventiva frente a las amenazas que sobre ellos se ciernen.

La puesta en marcha del Programa Nacional de Sondas requiere la implantación de una sonda individual en la red de cada Organismo adscrito al programa. Esta sonda es un servidor de alto rendimiento que se encarga de recolectar la información de seguridad relevante que detecta y, tras un primer filtrado, envía los eventos de seguridad hacia el sistema central, donde se realiza una correlación entre los elementos recogidos y entre los distintos dominios (organismos).

3.2.1.1. Diseño, producción y mantenimiento del Programa Nacional de Sondas

Los dos primeros años del Programa Nacional de Sondas se dedicarán a la planificación y diseño del programa. Esto implica tanto la creación del dispositivo de recolección de tráfico en las redes de cada organismo (es decir, el servidor con capacidad para capturar y procesar tráfico, denominado "sonda") como la conexión con la Plataforma de Agregación de Eventos (ver apartado 3.4), que es donde se almacenarán los datos para su posterior explotación.

La fase de diseño deberá ir seguida de la producción de dichas sondas de forma estandarizada. Así, se favorecerá la integración de las sondas en las redes de los organismos y el despliegue de forma fácil y controlada.

La producción de sondas vendrá acompañada de una actividad paralela que consistirá en proporcionar el mantenimiento y actualizaciones necesarias para garantizar que las sondas continúan funcionando correctamente, además de permanecer acordes a la evolución de la tecnología a lo largo de los años.

3.2.1.2. Despliegue y operación del Programa Nacional de Sondas

El despliegue de las sondas se llevará a cabo de acuerdo a las siguientes directrices:

[3] Sistema de Alerta Temprana (SAT), CCN-CERT: https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat/sat-inet.html

- En primer lugar, se deberá instalar la sonda en el organismo y hacer las configuraciones necesarias en la electrónica de red para enviar hacia la sonda el tráfico a analizar.

- La conexión entre la sonda y el sistema central se realizará siempre de forma segura, a través del establecimiento de un túnel cifrado. Dicha conexión puede realizarse a través de la salida a Internet del organismo adscrito, o a través de una salida dedicada hacia Internet. El túnel cifrado se establecerá directamente entre la sonda y el sistema central, de forma que no será necesaria ninguna infraestructura adicional por parte del organismo para proporcionar los túneles cifrados.

- La sonda se gestionará completamente desde el G-SOC, por lo que no será necesario que el personal del organismo realice tareas de administración. En ocasiones puntuales se solicitaría apoyo al organismo en caso de que ciertas tareas no pudieran realizarse de manera remota.

- Será el G-SOC quien esté a cargo de la gestión, actualización y mantenimiento del sistema central, así como de añadir nuevas funcionalidades y herramientas e integrar las reglas de detección (propias y externas). Estas reglas propias se generarán a partir de la información obtenida durante la investigación de otros incidentes de seguridad y a partir de la información recibida de otros organismos con los que se mantenga un intercambio de información referente a incidentes de seguridad.

3.2.2. Cibervigilancia Preventiva

La Cibervigilancia Preventiva es, junto al Programa Nacional de Sondas previamente desarrollado, otro de los elementos que forman parte de la capacidad de detección de amenazas pasiva.

Básicamente, consiste en adquirir una solución que continuamente rastree y analice información que pueda suponer una brecha de datos para el Gobierno de Argentina. En particular, se deberá monitorizar la publicación, venta, etc. de credenciales compartidas en actividades de ciberdelincuencia.

La identificación de usuarios, direcciones de correo electrónico y contraseñas comprometidas, así como el siguiente paso de alertar a tiempo sobre ello a la organización oportuna, es una medida preventiva clave para protegerse del impacto que produce la filtración de esta información. Por supuesto, este servicio debe ir acompañado de una política de generación y rotación de contraseñas adecuada para que el objetivo del servicio (evitar accesos no autorizados mediante credenciales exfiltradas) sea efectivo.

3.2.3. Plataforma de Agregación de Eventos

Con el objetivo de mejorar y optimizar el rendimiento del SIEM (ver apartado 4.1) así como de reducir los tiempos de búsqueda y de resolución de problemas, se implementará una plataforma de agregación de eventos que permita limitar la cantidad y mejorar la calidad de los diferentes eventos de seguridad recolectados que posteriormente alimentarán al SIEM.

Esta plataforma constituirá el punto central en el que se recolectarán, filtrarán, normalizarán y almacenarán los eventos de seguridad generados por las diferentes herramientas, sondas o sensores

desplegados en los organismos, lo que permitirá reducir significativamente el tamaño y la complejidad de los datos obtenidos.

3.2.3.1. Diseño y puesta en marcha de la Plataforma de Agregación de Eventos

Al constituir los diferentes eventos de seguridad recopilados información sensible y crítica para las organizaciones, se deberá garantizar su confidencialidad e integridad desde su generación en origen hasta la integración en la plataforma de agregación de eventos, estableciendo siempre que sea posible una red privada virtual (VPN) entre cada una de las organizaciones y la plataforma de agregación de eventos.

Durante la fase de diseño se deberán considerar las diferentes organizaciones que serán incorporadas a la plataforma, así como el número de dispositivos o eventos por segundo que cada una de ellas integrará en la misma, con el fin de dimensionar correctamente la plataforma.

3.2.3.2. Adquisición de la Plataforma de Agregación de Eventos

A la hora de adquirir la plataforma de agregación de eventos se deberá tener en cuenta que esta cuente con, al menos, las siguientes funcionalidades:

- Recolección e ingesta de gran cantidad de datos: La plataforma debe ser capaz de garantizar en todo momento una elevada tasa de ingesta de datos de una gran variedad de fuentes diferentes.
- Almacenamiento de datos seguro: La plataforma debe ser capaz de proporcionar un almacenamiento seguro de los datos con el fin de evitar el acceso no autorizado a los mismos.
- La plataforma debe ser compatible con el resto de los elementos de la arquitectura de seguridad para garantizar el correcto flujo de la información.

3.2.3.3. Despliegue, operación y soporte de la infraestructura tecnológica de la Plataforma de Agregación de Eventos

La plataforma de agregación de eventos deberá desplegarse en un punto de la red que sea alcanzable por todas las organizaciones que vayan a integrarse con ella.

Todos los eventos recibidos deberán ser clasificados permitiendo que se pueda identificar de forma rápida e inequívoca la fuente de la que proceden, el tipo de evento y el nivel de criticidad del mismo.

Los operadores designados para operar, administrar y gestionar la plataforma serán los encargados de integrar todas las fuentes que sean necesarias, así como de garantizar que la plataforma permite llevar a cabo las siguientes funciones correctamente:

- Deduplicación de eventos: La plataforma deberá ser capaz de integrar instancias similares de forma que se permita minimizar la cantidad de eventos procesados y almacenados.
- Correlación de eventos: El motor de correlación deberá ser capaz de encontrar relaciones simples entre eventos similares o de identificar una secuencia de eventos relacionados entre sí que desencadenen otro evento o alerta.

- Clasificación y filtrado de eventos: Con el fin de facilitar la tarea a los analistas, los eventos deberán ser normalizados y clasificados de forma que posteriormente se permita el filtrado por una serie de campos como la fecha y hora, la fuente (organización y dispositivo), la dirección IP o MAC, el nombre de equipo, o cualquier cadena específica que pueda existir en el evento.

3.2.4. Plataforma de Big Data

Es probable que, hacia el final del programa, el volumen de datos generados alcance dimensiones y complejidad suficientes como para tenga sentido que sean explotados mediante tecnologías Big Data. A medida que se implementen plataformas y servicios en distintos organismos, la cantidad de eventos relevantes para la seguridad puede crecer más allá de las capacidades con las que cuentan las herramientas de detección y respuesta tradicionales. La operación de tecnologías Big Data a gran escala requiere un profundo conocimiento técnico que no será trivial para los equipos comúnmente encargados de trabajar en el SOC o con el SIEM, por ejemplo. Además, y más importante, exigiría demasiado tiempo en tareas no directamente relacionadas con su cometido.

Por ello, una plataforma de Big Data[4] que venga alimentada por la Plataforma de Agregación de Eventos sumará ciertas ventajas que otros servicios quizá no puedan ofrecer. El inmenso universo que compone el mundo de la ciberseguridad (redes, dispositivos, aplicaciones, usuarios, artefactos y un largo etcétera) está en constante cambio, así que la representación de lo que sucede en el mismo, mediante el procesado de los eventos asociados a dicho universo, supone un activo muy valioso, ya que permite trazar su evolución temporal. Por supuesto, este valor se verá incrementado con el enriquecimiento de los datos desde otras fuentes.

La posibilidad de que se puedan practicar búsquedas de forma eficiente en un enorme corpus de datos de seguridad proporcionará a los analistas una conciencia situacional clave en el entendimiento, por ejemplo, de los comportamientos de los “threat actors” o en la contextualización de una serie de incidentes.

Para que todo ello sea operativo y funcional, es necesario que la plataforma se construya con tecnologías adecuadas al tamaño y naturaleza de los datos.

Aparte de las herramientas y tecnologías, la utilización efectiva de una Plataforma de Big Data pasa por establecer una serie de procesos de estructuración, limpieza, validación, clasificación, modelado y estandarización de los datos, además de ingestarlos y transformarlos adecuadamente para su uso útil en labores relacionadas con la ciberseguridad.

Las aportaciones de estos servicios de Big Data deben repercutir en un aumento de la calidad de la información con la que trabajan todos los equipos, y sobre todo en una mejora de la capacidad de detección del G-SOC en general e incluso de la capacidad de respuesta, cuando se desplieguen servicios más avanzados como Threat Hunting por ejemplo (ver apartado 5.3).

[4] Big Data Special Interest Group, FIRST: https://www.first.org/global/sigs/bigdata/

3.2.5. Implantación de SOAR

Las herramientas de orquestación, automatización y respuesta de seguridad o SOAR (Security Orchestration, Automation and Response) son productos de software que permiten a una organización responder a eventos de seguridad sin necesidad de asistencia humana, a partir de los datos que recogen sobre amenazas de seguridad.

Las acciones automatizadas se establecen en playbooks, ya sean predefinidos o personalizados. Si se produce un determinado suceso que activa un playbook, se pondrán en marcha los pasos que lo componen (bloqueos, alertas, acciones de investigación, reportes, etc.).

Los beneficios de implementar un SOAR van relacionados principalmente con mejoras en tiempos de detección y de reacción, escalabilidad y disminución de costes. Una vez integrada la plataforma de SOAR en los procesos de seguridad de la organización, se conseguirá simplificar la gestión de todo el sistema mediante una única interfaz centralizada.

Debe tenerse en cuenta, sin embargo, que estas plataformas no son una solución infalible ni un sistema que proteja por sí mismo. Es más bien una tecnología complementaria al resto de herramientas de seguridad, apropiada en una fase de madurez avanzada en seguridad, que no sustituye al resto de servicios de seguridad ni a los analistas humanos, pero sí potencia sus capacidades e incrementa su efectividad en detección de incidentes y respuesta.

3.2.6. Seguridad Ofensiva (Red Team)

Con el objetivo de poner a prueba la capacidad de detección y respuesta del SOC e identificar tanto sus fortalezas como especialmente sus debilidades, la capacidad de detección de amenazas activa contempla la actuación de un equipo de profesionales de seguridad especializados en seguridad ofensiva o Red Team.

Este equipo simulará las acciones llevadas a cabo por los cibercriminales durante una fase de ataque, con el objetivo de violar o comprometer la seguridad de la organización y a su vez evaluar cómo el equipo de seguridad de la organización responde a estas amenazas.

Durante una primera fase inicial, el Red Team evaluará la superficie de exposición de la organización y se centrará en la búsqueda de las diferentes vulnerabilidades que puedan existir, bien asociadas a sus activos digitales, activos físicos, procesos técnicos o procesos operativos.

Una vez identificadas estas debilidades y determinados los objetivos específicos de la prueba, el equipo iniciará la fase de ataque, en la que se llevará a cabo la explotación de las vulnerabilidades previamente identificadas. En paralelo, el SOC deberá ser capaz de identificar la actividad del Red Team como maliciosa y comenzar a contener, limitar y bloquear, si fuera posible, el ataque.

Una de las ventajas claras de este tipo de ejercicios es la oportunidad de evaluar las capacidades completas de la organización ante un ataque muy similar a uno real, poniendo el foco en elementos difíciles de explorar como la seguridad en los puestos de trabajo, la concienciación de los usuarios, los protocolos corporativos y la capacidad del SOC de detectar artefactos generados por la actividad del

Red Team tras el compromiso inicial (comunicación con servidores de comando y control, exfiltración de datos sensibles, etc.).

Tras la finalización del ejercicio, cada una de las partes deberá ser capaz de proporcionar una lista de hallazgos que muestren el valor de su perspectiva y del ejercicio en su conjunto, permitiendo mejorar las capacidades defensivas de la organización, así como la habilitad de detección y respuesta del SOC.

3.2.7. Análisis de Vulnerabilidades

En paralelo a las acciones desarrolladas por el equipo de seguridad ofensiva, se desarrollarán pruebas de penetración sobre redes, sistemas, aplicaciones, dispositivos, etc. con el objetivo de identificar y explotar el mayor número de vulnerabilidades posible para evaluar el nivel de riesgo asociado a ellas.

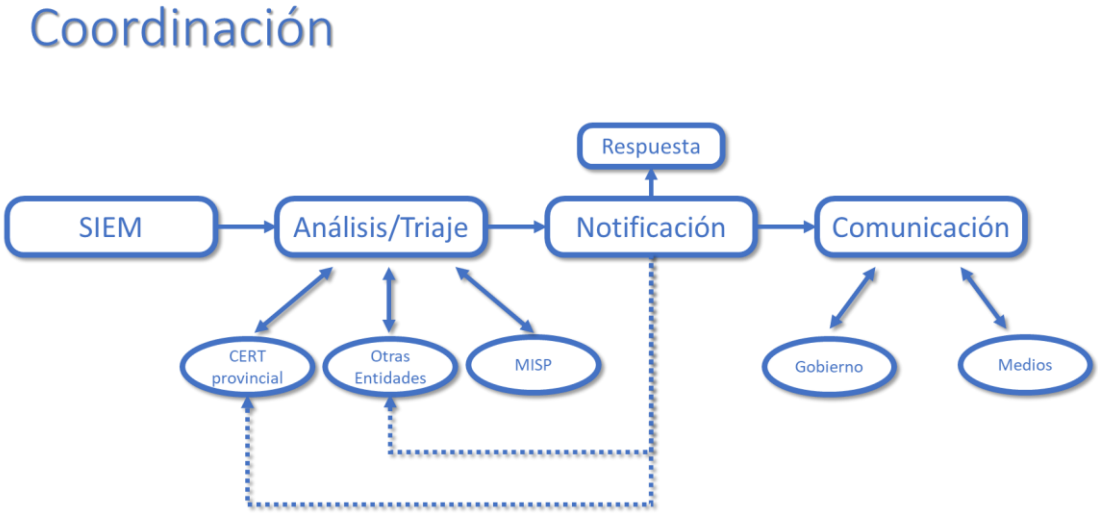
A diferencia de los ejercicios desarrollados por el Red Team, el análisis de vulnerabilidades no suele centrarse en el sigilo o la evasión, sino que busca un análisis general de la superficie de exposición, haciendo hincapié en los vectores comunes de entrada.

Este tipo de análisis permiten al equipo de seguridad identificar de manera directa la superficie de exposición, evitando puntos ciegos, configuraciones erróneas y en general asegurar que el equipo de seguridad cuenta con información veraz y actualizada sobre el estado de la infraestructura.

4. Servicios de la Capacidad de Coordinación

La Capacidad de Coordinación dispondrá de una mayor cantidad de operadores o analistas, ya que conforma la actividad central del G-SOC. Estos equipos desarrollarán dicha capacidad en sus distintas etapas. La parte más importante de la Capacidad de Coordinación será su sección de operaciones, pero también contará con una sección de análisis de riesgo y estará conectada con la oficina de seguridad, dedicada a temas de desarrollo normativo, cumplimiento y formación.

A partir de los datos recogidos en la Plataforma de Agregación de Eventos y consolidados en la plataforma SIEM, se realizarán las operaciones de la Capacidad de Coordinación. En primer lugar, se determinará si lo que se ha detectado conforma un incidente, y en tal caso se notificará. A continuación, el incidente pasará tanto a los equipos de la Capacidad de Respuesta como al servicio de comunicación, que trasladará la información de manera adecuada al Gobierno y a los medios.



4.1. SIEM

Los miles de eventos diarios generados en las organizaciones adscritas al G-SOC deben ser revisados para discriminar cuáles son realmente importantes. Para ello se hará uso de una solución SIEM (Security Information and Event Management), que monitorice y recoja eventos del entorno IT de los organismos, una vez hayan sido centralizados en la Plataforma de Agregación de Eventos (ver apartado 3.2.3).

Partiendo de los datos ya filtrados y normalizados que proporciona la Plataforma de Agregación de Eventos, la operativa sobre los eventos de seguridad volcados en el SIEM será más simple y efectiva. Se les aplicarán reglas de correlación que identifiquen posibles usos indebidos o anomalías y alertará a los analistas en caso de detectar una situación de riesgo.

4.1.1. Adquisición de la infraestructura tecnológica SIEM para el CERT / G-SOC

La plataforma SIEM por la que se opte debe tener al menos las siguientes funciones básicas[5]:

- Agregación de información. Debe permitir agregar logs provenientes de múltiples fuentes como dispositivos de red, dispositivos de seguridad, servidores, bases de datos, aplicaciones, etc., y que dicha información sea consolida con el objetivo de evitar la pérdida de eventos importantes.

- Correlación de eventos. Esto implica la búsqueda de atributos comunes entre eventos procedentes de múltiples fuentes y la capacidad de relacionarlos entre sí para convertir los datos recogidos en información útil.

- Generación de alertas. Se requerirá poder notificar a un conjunto de destinatarios de los sucesos de interés de manera inmediata, mediante la automatización del análisis de eventos correlados y la generación de alertas.

- Visualización con dashboards. Se hará uso de representaciones visuales de los datos de los eventos procesados, para simplificar la tarea del analista en el análisis de patrones o identificación de actividad anómala respecto a las características habituales.

- Conformidad con políticas (*compliance*). Las herramientas SIEM pueden emplearse para automatizar el proceso de recogida de datos de conformidad con las políticas que se hayan establecido, para así generar informes adaptados a los procesos existentes de seguridad, gobernanza y auditoría.

- Retención. El requerimiento de almacenar un histórico de datos durante grandes periodos de tiempo está directamente relacionado con permitir la correlación de información a lo largo del tiempo y también con el cumplimiento de requisitos de conformidad existentes. Además, afecta de manera crucial al siguiente punto: las investigaciones forenses.

[5] Gestión de Incidentes de Ciberseguridad, Moreno García: ISBN 9788418971730

- Análisis forense. Un SIEM ofrece la posibilidad de buscar de manera centralizada a través de los logs de diferentes elementos en el periodo temporal establecido, por ejemplo, durante la gestión de un incidente. Haber preservado todos los eventos relevantes correctamente será crítico para que una investigación forense llegue a buen término, ya que lo normal es que el descubrimiento de una brecha de seguridad se produzca tiempo después de que se haya producido.

4.1.2. Operación L1-L2 sobre el SIEM del CERT / G-SOC

Por operación L1 nos referimos al primer nivel de soporte consistente en la clasificación del incidente y su resolución en el caso de que exista un procedimiento probado para ello.

Por operación L2 nos referimos a la proporcionada por personal con mayor experiencia que sólo atenderá aquellos incidentes escalados por el nivel L1, cuya complejidad haya hecho imposible su resolución en el primer nivel.

La explotación del SIEM se llevará a cabo por un equipo de analistas especializados, que serán el núcleo de las actividades del Centro de Operaciones de Seguridad o SOC. Este grupo de profesionales se encargará de monitorizar la seguridad de los sistemas de información a proteger, detectando y trabajando por detener los incidentes de seguridad que se produzcan.

El SOC prestará los servicios principalmente de análisis y triaje de los eventos de seguridad, que serán sus actividades más importantes. Adicionalmente, los servicios que componen su trabajo se enmarcan en las cinco áreas que define la organización FIRST (Forum of Incident Response and Security Teams) en su framework de servicios de un CSIRT[6]:

- Gestión de los eventos de seguridad (Information Security Event Management): en esta área se engloban los servicios de monitorización y detección, así como el análisis de eventos. Este último servicio incluye la función de correlación, cuyo propósito es la identificación de eventos directamente relacionados con otros incidentes de seguridad potenciales o en curso.

- Gestión de incidentes de seguridad (Information Security Incident Management): este área, que es el corazón de cualquier CSIRT, comprende los servicios de análisis y gestión de incidentes, mitigación de ataques y actuación ante incidentes en coordinación con los servicios de la capacidad de respuesta (ver apartado 5).

- Gestión de vulnerabilidades (Vulnerability Management): en el caso del G-SOC de Argentina, las funciones de esta área corresponden a un servicio independiente, dentro de la capacidad de Detección de Amenazas Activa (ver apartado 2.7), pero es conveniente que los resultados de dicho servicio se integren con la información de la que dispone el SOC.

- Conciencia situacional (Situational Awareness): es la habilidad de identificar, procesar, comprender y comunicar los aspectos relevantes de qué está ocurriendo alrededor del área de responsabilidad

[6] Computer Security Incident Response Team (CSIRT) Services Framework, FIRST: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

del G-SOC que pueda afectar a su operación o misión. Esto incluye tanto ser consciente del estado actual como identificar o anticipar potenciales cambios. Dependiendo de la organización, a veces se dedica un equipo separado para estas tareas de recoger e integrar información y distribuirla de manera oportuna, mientras que otras veces es el equipo del CSIRT quien lo provee en base a su visibilidad y entendimiento del contexto. En el caso del G-SOC de Argentina, estas funciones se reparten con la Detección de Activos y de Amenazas, por un lado, y con la Plataforma de Notificación y la Consultoría de Comunicación, por el otro, pero dichas actividades deberán estar alineadas con el SOC para que este complete su conciencia situacional.

- Transferencia de conocimientos (Knowledge Transfer): también pertenece al SOC la responsabilidad de crear las mejores prácticas operacionales posibles para ayudar a la organización a detectar, prevenir y responder ante incidentes de seguridad. La puesta en práctica de ejercicios, formaciones y recomendaciones técnicas es clave para la mejora continua de su ciberseguridad.

La organización de un SOC viene dada por varios niveles, según su grado de especialización y formación. Cada nivel tiene unas funciones asignadas. Los modelos más habituales son el de tres capas y el de dos capas. En el de tres capas, las responsabilidades están más estratificadas y aparece una separación mayor, para poder incorporar analistas junior de manera efectiva y que los costes y habilidades del equipo estén mejor balanceados.

Sin embargo, en el caso del G-SOC de Argentina se ha entendido que el modelo de dos capas (L1-L2) cubrirá mejor las necesidades a las que se pretende responder. Este modelo, más sencillo, se divide en dos líneas. La primera línea está compuesta por analistas de seguridad con cierta experiencia, capaces de monitorizar el SIEM, dar soporte inicial, generar informes, cerrar algunos casos basados en criterios bien definidos y escalar los casos más difíciles o complejos tras haber recogido la información clave de los mismos. En la segunda línea se sitúan especialistas de nivel de ingeniería que atenderán los casos más complejos o que requieran análisis más profundos, además de que serán el nivel que coordine la gestión de incidentes.

4.2. Plataforma Nacional de Notificación y Coordinación de Incidentes

Con el fin de mejorar y facilitar la coordinación entre el CERT Gubernamental Nacional, el G-SOC y los distintos organismos y organizaciones, es necesario desarrollar una Plataforma Nacional de Notificación y Coordinación de Incidentes de Seguridad.

Esta herramienta permitirá agilizar los procedimientos de gestión y notificación de los incidentes, al agregar en una única plataforma ambos procesos, y permitiendo a su vez el intercambio de información técnica entre todas las partes involucradas, limitando el alcance e impacto del incidente en curso.

La plataforma deberá ofrecer un lenguaje común para la clasificación de los incidentes y de los niveles de amenaza y notificar en tiempo real a todas las autoridades competentes, lo cual permitirá no solo

facilitar el seguimiento y la trazabilidad del caso, sino también asignar a éste los recursos necesarios en el menor tiempo posible.

Además de limitar el impacto del incidente en curso, esta plataforma de notificación permitirá alertar a otros organismos, a priori no involucrados o afectados, sobre las ciberamenazas activas en ese momento. El intercambio de información en tiempo real podrá ayudar a prevenir que un incidente acabe afectando a más de un organismo y permitirá a su vez conocer el estado real de la ciberseguridad a nivel nacional, facilitando a las autoridades la toma de decisiones y el desarrollo de nuevos planes o protocolos de actuación si fuera necesario.

4.3. Plataforma Nacional de Intercambio de Información de Amenazas

El intercambio de información es un aspecto crítico y fundamental de la gestión de la ciberseguridad. Este punto sumado a la colaboración entre las diferentes organizaciones y entidades es lo que ha permitido en los últimos años un desarrollo constante que permita contrarrestar el avance continuo de los cibercriminales.

Es por ello que el desarrollo de una Plataforma Nacional de Intercambio de Información de Amenazas es imprescindible para proteger los intereses políticos, económicos, industriales, comerciales y estratégicos de Argentina.

Bajo el principio de cooperación, esta plataforma permitirá dar una respuesta coordinada a los incidentes de seguridad, consiguiendo una actuación ágil y eficaz que permita proteger y defender a los organismos adheridos, limitando por un lado el impacto y alcance que las ciberamenazas puedan generar y permitiendo, por otro lado, elaborar un mapa sobre la situación de la ciberseguridad a escala nacional.

EL Departamento de Seguridad Nacional de los Estados Unidos de América lideró, junto a organismos como el US-CERT y MITRE, la creación de un marco común para el intercambio de información sobre ciberseguridad compuesto fundamentalmente por los estándares STIX y TAXII.

- **STIX (Structured Threat Information eXpression)**: Es un lenguaje común, estructurado, en formato XML, para la especificación y caracterización de información sobre amenazas de ciberseguridad

- **TAXII (Trusted Automated eXchange of Indicator Information):** Este estándar tiene como fin definir las especificaciones de un mecanismo de transporte de mensajes que permita a las organizaciones y a los sistemas de información el intercambio de información sobre ciberamenazas. La información deberá ser descrita preferiblemente empleando el estándar STIX, previamente definido.

Estos estándares, creados con una orientación internacional y completamente libre, permiten la automatización del intercambio de información sobre ciberseguridad en tiempo real.

La Plataforma Nacional de Intercambio de Información de Amenazas deberá comunicarse con las plataformas de CERTs provinciales y otras entidades, de manera que la información quede interconectada y en definitiva se apliquen los principios de cooperación expresados anteriormente.

4.4. Consultoría de Análisis de Riesgos

El análisis de riesgos informáticos es un proceso a través del cual se identifican las vulnerabilidades y amenazas a las que están expuestas los activos informáticos, así como su probabilidad de ocurrencia y el impacto que las mismas generarían, con el fin de determinar la asignación de recursos (técnicos o de otro tipo) necesarios para asumir el riesgo real al que se expone tanto la información como los sistemas.

Con el fin de conocer el riesgo al que están sometidos los elementos de trabajo que permita habilitar un marco equilibrado de Gobierno, Gestión de Riesgos y Cumplimiento (GRC) de forma que se consiga en la organización evitar conflictos, duplicación de actividades y zonas de nadie, se propone la implementación de herramientas EAR (Entorno de Análisis de Riesgos) basadas en la metodología Magerit.

Esta metodología (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) implementa el proceso de gestión de riesgos dentro de un marco de trabajo que facilite a los órganos de gobierno la toma de decisiones que permitan mitigar los riesgos.

Sus objetivos, directos e indirectos son:

- Concienciar a los responsables de las organizaciones sobre la existencia de riesgos y de la necesidad de su gestión.
- Ofrecer un método que permita analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones.
- Ayudar a descubrir y planificar el tratamiento necesario para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Magerit ofrece una guía completa (dividida en 3 volúmenes) sobre cómo abordar el análisis de riesgos. El primero de ellos se centra en el método y en él se describe la estructura que debe tener el modelo de gestión de riesgos. El segundo de ellos es un catálogo de elementos que marca unas pautas en cuanto a los tipos de activos, los criterios para su evaluación, las amenazas típicas sobre los sistemas de información y las salvaguardas a considerar para proteger estos sistemas. El último libro es una guía de técnicas en el que se describen las diferentes técnicas habitualmente utilizadas en el análisis de riesgos.

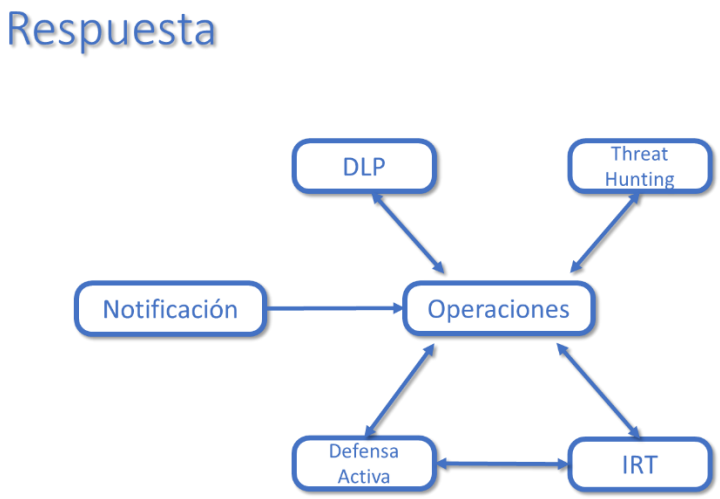
4.5. Consultoría de Comunicación

Una parte importante de la gestión de un incidente es cómo se comunica hacia las distintas partes interesadas. Escoger qué es relevante para cada receptor, cuándo se debe comunicar, de qué modo, etc. es una responsabilidad suficientemente sensible como para requerir un servicio profesional dedicado a ello.

Este servicio de consultoría de comunicación será el encargado de mantener informados tanto al Gobierno de Argentina como a los medios que publiquen noticias sobre incidentes de ciberseguridad en las administraciones de Argentina, adecuando el mensaje para ambos casos. Deberá actualizar el estado del incidente para que quienes deban tomar decisiones estén correctamente informados en todo momento, y así contribuir a un mejor manejo del incidente.

5. Servicios de la Capacidad de Respuesta

En el extremo final del flujo que siguen las Capacidades Nacionales, encontramos la Capacidad de Respuesta, que lógicamente será aquella con la que se mitiguen los incidentes. Dentro de esta capacidad encontramos distintos equipos que se dedican a diversas tareas, explicadas a continuación.



5.1. Defensa Activa

Frente a un incidente confirmado, se tiene que tener la capacidad de adaptar las medidas defensivas de forma adecuada. No solo en caso de sufrir un ataque directo, sino como respuesta a la información recibida por los incidentes sucedidos en otras entidades conectadas con el G-SOC.

Esto quiere decir que en la capacidad de respuesta debe existir un componente relevante de defensa activa. Esto es, se deben definir competencias y establecer procesos y dedicaciones para que, ante la recepción de IOCs (Indicators of Compromise) vía por ejemplo la Plataforma Nacional de Intercambio de Información de Amenazas (ver apartado 4.3), estos se distribuirán de forma pertinente en los sistemas y herramientas que corresponda. De esta manera, la protección de los activos tecnológicas permanecerá actualizada y podrá anticiparse a campañas o nuevos ataques que estén ocurriendo en tiempo real. También incluirá la aplicación de políticas de seguridad en los equipos perimetrales, sistemas de protección del endpoint, equipos de red o allá donde se puedan incorporar medidas preventivas como defensa ante amenazas en constante evolución.

5.2. IRT (Incident Response Team)

El equipo de respuesta a incidentes es el grupo de la organización responsable de desarrollar las tareas necesarias para prevenir, gestionar y responder ante un incidente de seguridad. Entre sus objetivos principales se encuentran los siguientes:

- Verificar si el incidente de seguridad ha ocurrido o no, documentándolo en este segundo caso.
- Mantener o restaurar la continuidad del negocio, a la vez que se reduce el impacto del incidente.
- Identificar la causa del incidente.
- Mantener informados a los grupos necesarios (gerencia, personal) sobre la situación actual y la respuesta que se está llevando a cabo.
- Aplicar las medidas de seguridad necesarias para evitar o minimizar el impacto de futuros incidentes.
- Documentar las lecciones aprendidas.

5.3. Threat Hunting

Se conoce como *Threat Hunting* al proceso proactivo que asume que existe alguna intrusión o violación de la seguridad de la organización con el fin de identificar amenazas de seguridad previamente desconocidas o en curso sin remediar.

El *Threat Hunting* va más allá de las tecnologías de detección tradicionales como los SIEM o los EDR, analizando los datos de seguridad recolectados y buscando patrones de actividad sospechosa con el fin de obtener información procesable. Se trata de una tarea muy disciplinada que comienza con el establecimiento de una hipótesis comprobable (basada en datos). Esta hipótesis es posteriormente analizada utilizando todas las fuentes de información disponibles, adoptando un enfoque longitudinal de las alarmas, los eventos y la actividad generada e incorporando la información sobre el estado actual de la red y los sistemas, de forma que el análisis contra esas líneas base conocidas permita localizar potenciales amenazas de una manera mucho más efectiva.

Entre los muchos beneficios que el *Threat Hunting* aporta a la organización encontramos los siguientes:

- Maximizar la inversión en seguridad a través de la extracción de datos, el análisis, la generación de informes y la mejora de los sistemas de alerta.
- La revisión y el análisis por parte de los profesionales de seguridad permite definir líneas base sobre las operaciones de los sistemas o de la red (volumen o velocidad de tráfico, patrones de flujo de datos, etc.) permitiendo detectar con mayor facilidad desviaciones respecto a las operaciones normales.

- Detección e identificación más rápida y eficaz de los atacantes, reduciendo el tiempo de permanencia de los mismos en la organización, evitando daños mayores y limitando el impacto de la amenaza.

5.4. Mitigación de Denegación de Servicio Distribuida

Un ataque de denegación de servicio distribuido (DDoS) es una técnica malintencionada utilizada por los cibercriminales cuyo propósito consiste en interrumpir el funcionamiento normal de un servidor, servicio o red, sobrecargando el objetivo o la infraestructura del mismo mediante una avalancha de tráfico desde internet. El indicio más claro de este tipo de ataques es la ralentización o inaccesibilidad de un servicio.

Con el fin de evitar que este tipo de ataques puedan causar graves consecuencias en los sistemas, se propone la implementación de un servicio de mitigación DDoS que permita no solo detectar sino también desviar, filtrar y analizar el tráfico, con el fin de mitigar el ataque.

5.5. Detección de Fuga de Información

La información constituye uno de los bienes intangibles de mayor valor y más críticos para las organizaciones. Es por ello que hoy en día las fugas de información son una de las mayores amenazas a las que tenemos que enfrentarnos.

La protección de la información se articula en torno a tres principios básicos: confidencialidad, integridad y disponibilidad.

- Confidencialidad: Implica que la información sea accesible únicamente por el personal autorizado para ello.
- Integridad: Garantiza la exactitud de los datos, asegurando que estos no han sido alterados.
- Disponibilidad: Implica que la información sea accesible en todo momento.

Las fugas de información son incidentes en los que se ve afectado el principio de confidencialidad, es decir, cuando personas no autorizadas consiguen acceso a la información.

Con el fin de detectar y evitar la fuga de información debemos, por un lado, desarrollar y mantener actualizadas las políticas de acceso y, por otro lado, implementar las medidas técnicas necesarias como las soluciones DLP (*Data Loss Prevention*), que clasifican la información y permiten identificar las violaciones de las políticas definidas por la organización.

Estas herramientas supervisan y controlan las actividades de los equipos, analizando e inspeccionando los flujos de datos en la red corporativa con el fin proteger los datos en reposo, en movimiento y en uso.

Disponen además de alertas, cifrado y otras acciones de protección para evitar que los usuarios finales compartan o accedan a la información de manera accidental o maliciosa.