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

G-SOC: Qué es y para qué sirve.

Referencia del Proyecto

OP22-0472

Versión: 1.10

Estado: Aprobado
Fecha: 08/07/2022

Autores
Equipo CSA

Cliente

BANCO INTERAMERICANO DE DESAROLLO

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	01/06/2022		Borrador inicial.
0.6	24/06/2022		Borrador completo para revisión.
0.9	30/06/2022		Figura añadida.
0.10	07/07/2022		Añadidos puntos "*7. Status global de ciberseguridad en la APN*", antes en doc separado, y ""
1.10	08/07/2022		Aprobado.

Índice

1. Introducción 4

2. Concepto de Centro de Operaciones de Ciberseguridad SOC 6

2.1. Marco de referencia del SOC: PPTGC 7

3. Delimitación del concepto de SOC 8

4. Funciones y servicios del G-SOC 9

4.1. Servicios de Prevención 9

4.2. Servicios de Protección 9

4.3. Servicios de Detección 10

4.4. Servicios de Respuesta 10

4.5. Servicios de Asesoramiento 10

5. Componentes del SOC 11

5.1. Personal 11

5.1.1. Roles de gestión 11

5.1.2. Roles técnicos 12

5.1.3. Roles consultivos 12

5.1.4. Personal externo 12

5.2. Procesos 13

5.2.1. Preparación 13

5.2.2. Detección y analisis 14

5.2.3. Contención, erradicación y recuperación 15

5.2.4. Actividad post-Incidente 15

5.3. Tecnología 16

5.4. Gobernanza y cumplimiento 17

6. Retos 18

7. Status global de ciberseguridad en la APN 19

8. Justificación para el despliegue de un G-SOC 22

ANEXO: Lista de acrónimos en el documento 23

1. Introducción

Según un informe reciente[1], el promedio de **brechas de seguridad reportadas por las organizaciones aumentó** un 11 %, de 2017 a 2018. En los años de 2015 a 2020, este número creció un total del 65%. El informe solo cubrió los incidentes detectados y notificados, y es seguro que el número de incidentes no notificados fue muy superior.

El coste anual de cualquier tipo de ciberataque también crece a un ritmo constante. Y muchos ataques pasan desapercibidos durante demasiado tiempo, lo que empeora el panorama. El tiempo medio para detectar un incidente fue de 196 días en 2018, y se necesitaron otros 69 días de media para paliar una brecha de seguridad, lo que **demuestra cuán ineficaces son las organizaciones para detectar y mitigar los ataques cibernéticos**.

Las razones de tal ineficiencia incluyen, entre otras:

- Carencia de una **visión general** de los dispositivos, sistemas, aplicaciones y redes por parte de las propias organizaciones.
- No saber **qué activos proteger**.
- Ignorar **qué herramientas usar** y cómo integrarlas con la infraestructura existente.
- Sentirse desbordado por la velocidad de **evolución de la tecnología** y el panorama de **amenazas**.

En los dos últimos años, el COVID-19 ha **acelerado aún más la transformación digital** de nuestras sociedades, y la ciberseguridad ha pasado a ocupar un lugar central entre las preocupaciones del mundo. Según otro estudio realizado por *Enterprise Insight* en 2020, el 78% de los líderes de TI (Tecnologías de la Información) considera que sus organizaciones no cuentan con las medidas apropiadas de ciberseguridad. De acuerdo al *Global Risk Report*[2] del Foro Económico Mundial, **la ciberseguridad se ubica entre los cinco riesgos más importantes** que enfrentan las empresas.

La **Protección de las Infraestructuras Críticas de Información**[3] (CIIP por sus siglas en inglés) es uno de los deberes de las naciones. Un incidente de ciberseguridad en estas Infraestructuras podría tener un gran impacto en la calidad de vida de los ciudadanos.

La SIT de la Jefatura de Gabinete de la República Argentina, junto con el BID está en fase de diseño de la operación de préstamo: *Programa de Ciberseguridad para Infraestructuras Críticas de Información*

[1] The Cost of Cybercrime, Accenture and Ponemon Institute, New York, NY, USA, 2018.
[2] http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[3] Infraestructura de información crítica es cualquier dato, base de datos, red, infraestructura de comunicaciones (o parte de ella), o cualquier cosa asociada con ellos que haya sido declarada como CII.

(ICI) AR-L1343, la cual tiene como objetivo el fortalecimiento de las capacidades del país para gestionar la ciberseguridad de sus ICI[4].

Dicho proyecto incluye la creación de un SOC[5] de gobierno (G-SOC) el cual será gestionado por dicha secretaría.

Los **ataques de seguridad son cada vez más complejos** y exhiben capacidades cada vez más sofisticadas. Por lo tanto, abordar la complejidad y sofisticación de tales ataques debe incluir no solo invertir en **medidas preventivas**, sino también el desarrollo de **capacidades de monitoreo inteligente** e integradas en un programa de **respuesta a incidentes**.

Podría decirse que verse comprometido en algún momento es inevitable. Como dijo un CEO de una importante compañía del sector de las TIC: "Hay dos tipos de organizaciones: las que han sido pirateadas y las que aún no saben que han sido pirateadas". Una brecha de seguridad no es un "si…", sino un "cuándo"; descubrir/anticipar y prevenir las brechas de seguridad es una de las muchas razones por las que las organizaciones desarrollan un SOC.

Aunque son unidades intrínsecamente centralizadas que se nutren de **datos de toda la organización**, los SOCs pueden ejercer funciones consultivas, emitir recomendaciones no vinculantes, ofrecer servicios no necesariamente de uso obligado. Sus funciones, carácter y encaje han de ser **coherentes con la idiosincrasia de la organización** a la que prestan servicio, so pena de estar abocadas al fracaso.

El concepto de SOC es amplio y flexible y su papel en la organización debe adecuarse a ella. La necesidad de defenderse de los ataques cibernéticos y robos de información, obliga a **identificar y subsanar las deficiencias de seguridad, establecer estrategias de defensa y disponer de herramientas y servicios para ello**. Facilitar esto, es la misión fundamental del SOC.

En este documento, se describe también, de forma breve, la **situación actual en relación a la ciberseguridad en la Administración Pública Nacional** de Argentina en su conjunto, en aquellos aspectos que pudieran **influir en el diseño y despliegue de un Centro de Operaciones de Ciberseguridad Gubernamental** (G-SOC AR).

También se apuntan **las razones por las que el despliegue de un G-SOC**, diseñado para proporcionar servicios y asesoramiento en ciberseguridad de forma transversal a los organismos de la APN que los requieran, y colaborando en la prevención, protección, detección y respuesta a amenazas e incidentes de ciberseguridad, **es considerado muy recomendable**.

[4] ICI, Infraestructuras Críticas de Información, activos informáticos que son esenciales para el funcionamiento de la sociedad y/o la economía.
[5] SOC: Security Operations Center, o Centro de Operaciones de Seguridad (también se usa el término ISOC, Information Security Operations Center).

2. Concepto de Centro de Operaciones de Ciberseguridad SOC

La importancia creciente de los SOCs en los últimos años, responde a la necesidad esencial de prevenir incidentes cibernéticos importantes. Como resultado, se adoptan operaciones de seguridad coordinadas, tanto en instituciones gubernamentales, como en compañías y negocios.

El objeto del G-SOC será la **prestación de servicios transversales de ciberseguridad a las entidades de la administración Pública Nacional (APN)**, que aumenten la capacidad de vigilancia y detección de amenazas en las operaciones diarias de los sistemas de información y comunicaciones de los diferentes organismos, así como la mejora de su capacidad de respuesta a ataques: su misión es la **de contribuir en la defensa de los sistemas de información**.

La siguiente figura ilustra la arquitectura, con las actividades más comunes de un SOC en la monitorización y análisis continuo para la protección de la organización a ataques avanzados de ciberseguridad, según modelo publicado por *Gartner, Inc* en febrero de 2014:

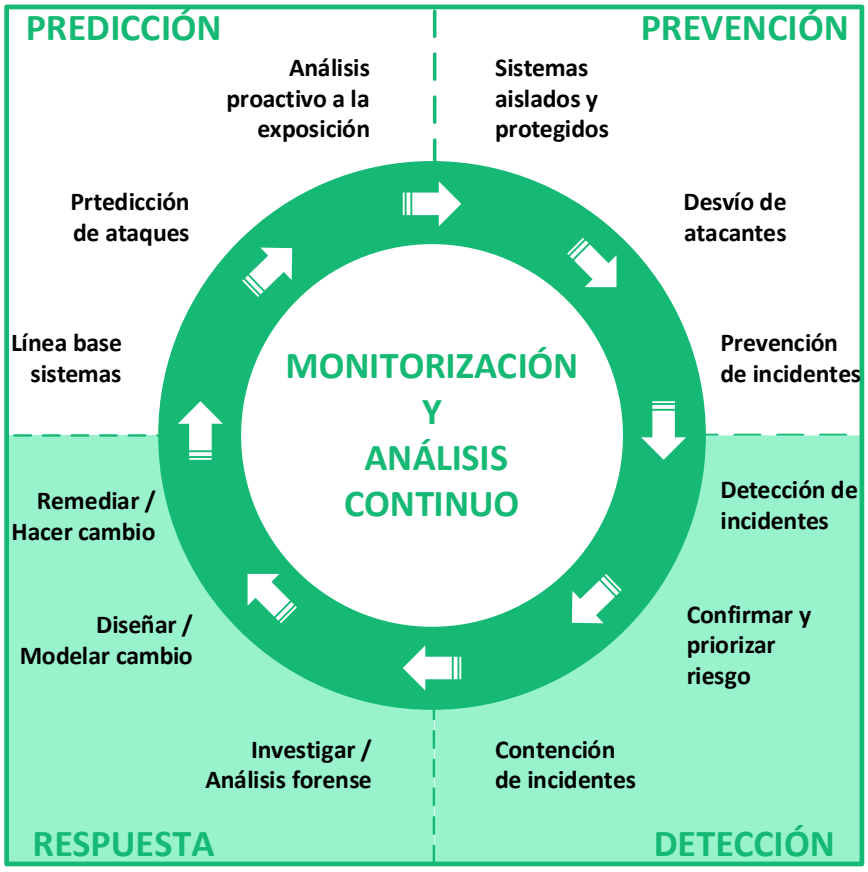

Ilustración 1. Diseño de una arquitectura adaptativa de seguridad para protección de ataques avanzados. (Gartner, Inc, febrero de 2014)

2.1. Marco de referencia del SOC: PPTGC

El SOC correctamente implementado, proporcionará una solución integral para detectar y mitigar ataques. Su actuación comprende a **las personas, los procesos y las tecnologías que monitorean y valoran la situación a través de la detección, contención y reparación de amenazas de TI para gestionar y mejorar la seguridad de una organización**. El SOC tratará cualquier incidente informático sospechoso de constituir una amenaza y asegurará que sea identificado y analizado, se comunique, se investigue y se informe adecuadamente. Cuidará de las aplicaciones para identificar un posible ciberataque o intrusión (evento) identificando si se trata de una amenaza maliciosa genuina (incidente) y si podría impactar la actividad y desempeño de la organización.

El **cumplimiento** se sustancia en garantizar que todas las actividades cumplan con los requisitos legales y reglamentarios, en adherirse a las **políticas y regulaciones**, micro y macro. La **gobernanza** es clave para la **alineación de procesos y la operación con el "cumplimiento"** de la normativa.

La siguiente figura ilustra el marco de referencia de forma gráfica:

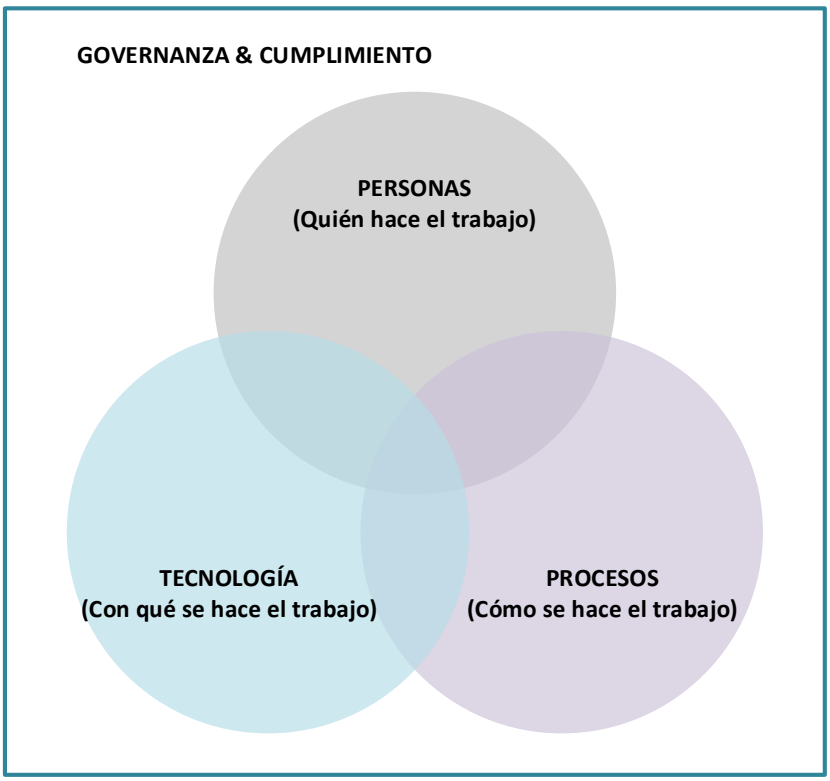

Ilustración 2. Marco de referencia del SOC: Personas, procesos y tecnología; Gobernanza y cumplimiento (PPTGC) [6].

[6] G. D. Bhatt, ``Knowledge management in organizations: Examining the interaction between technologies, techniques, and people,'' J. Knowl. 2001.

3. Delimitación del concepto de SOC

El término SOC es **amplio y flexible**, adquiriendo matices diferentes según la organización que lo implementa. Aunque el SOC se define como una unidad donde se supervisan, evalúan y defienden los sistemas de información de una organización (sitios web, aplicaciones, bases de datos, centros de datos y servidores, redes, equipos de escritorio y otros puntos finales), debe distinguirse de otras unidades con los que puede confundirse, tales como los CSIRT/CERT y NOC.

- CSIRT[7]. Equipo de Respuesta a Incidentes de Seguridad Informática (CERT[8])

  CSIRT a menudo se usa indistintamente para un SOC, aunque un CSIRT se centra esencialmente en la respuesta al ataque una vez que se ha producido. Un CSIRT es una unidad organizativa responsable de **coordinar y apoyar la respuesta a un incidente de seguridad informática**. Puede ser un **equipo independiente o parte de un SOC**.

  En lugar de CSIRT también se usa el término CERT (Equipo de Respuesta a Emergencias Informáticas). El nombre CERT fue usado originalmente por el CERT/CC y está registrado como marca comercial y de servicio por la Universidad Carnegie Mellon (CMU) en varios países. CMU fomenta el uso de CSIRT como término genérico.

- CERT AR

  Actualmente **existe en la Argentina el CERT AR** dependiente de la Secretaria de Innovación Tecnológica Publica SIT, que asiste en la gestión y manejo de incidentes de ciberseguridad en las entidades de la APM y ofrece asesoramiento cuando así se solicita por parte de estas.

  La creación de un G-SOC implicará que se defina el **status de ambos organismos**: muchos CSIRT/CERT han devenido en SOC de sus organizaciones con el paso del tiempo y la ampliación de funciones., pero otros modelos también son corrientes, como pasar a formar parte uno de otro, o mantener una relación autónoma, aunque con cierto grado de coordinación.

- NOC[9]. Centro de Operación de Red

  Un Centro de operaciones de red (NOC) supervisa la identificación, investigación, priorización, escalamiento y resolución de problemas. Sin embargo, en los NOC, los problemas abordados son diferentes, ya que el **NOC se enfoca en los incidentes que afectan el rendimiento y la disponibilidad de la red de una organización**. Dado que los incidentes pueden ocurrir en todos los sistemas, no solo en las redes, es beneficioso para las organizaciones que los equipos de NOC y SOC trabajen juntos.

[7] Computer Security Incident Response Team o CyberSecurity Incident Response Team
[8] Computer Emergency Response Team,
[9] Network Operations Center

4. Funciones y servicios del G-SOC

Desde el punto de vista de los servicios que un G-SOC debiera estar en disposición de ofrecer a las entidades de la APN en caso de máximo desarrollo, podemos agruparlas en las siguientes grandes cinco categorías, en las que se muestra para cada una un conjunto de los servicios más comunes:

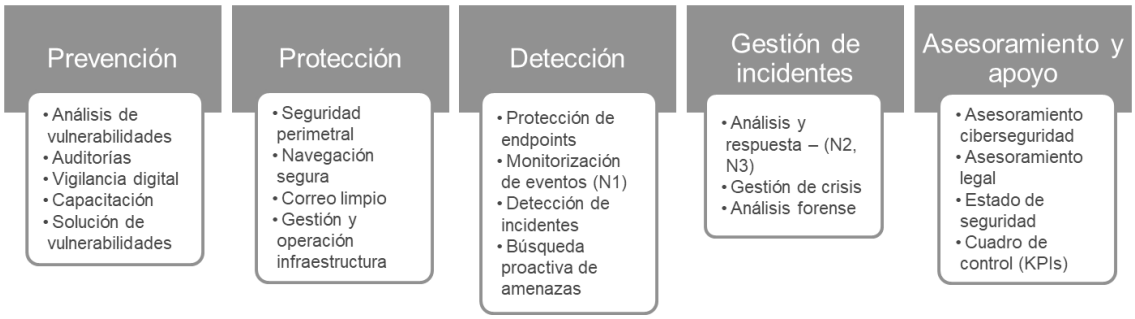

Ilustración 3. Categorías de los servicios del G-SOC.

4.1. Servicios de Prevención

El objetivo es conocer el **estado de la seguridad en el organismo**.

Ejemplos:

- Bajo demanda, el análisis de código en línea, así como análisis de las aplicaciones.
- Servicios de vigilancia digital.
- Formación y concienciación en seguridad.
- Soporte para la remediación de las vulnerabilidades detectadas.

4.2. Servicios de Protección

El objetivo es la **protección perimetral**.

Posibilidad de activar medidas en conjunto y mejora en detección de ciberataques.

Servicios tipo:

- Seguridad perimetral
- Navegación segura

- Correo limpio
- Acceso remoto seguro

4.3. Servicios de Detección

El objetivo es la **reducción del tiempo de detección de ataques** cibernéticos.

Ejemplos:

- Gestión de los EDRs y su instalación.
- Monitorización de los eventos de seguridad y detección de los posibles incidentes.
- Búsqueda de intrusiones; detección de fuga de información.
- Servicio de sondas.

4.4. Servicios de Respuesta

El objetivo es **mejorar la respuesta** ante ciber incidentes.

Ejemplos:

- Coordinación de medidas en caso de crisis.
- Servicio de análisis forense.
- Análisis de malware que se compartirá con las entidades.
- Para mejorar la detección, análisis del tráfico.

4.5. Servicios de Asesoramiento

El objetivo es **apoyar a las entidades en** asuntos relacionados con **ciberseguridad**.

Servicios de asesoría en:

- En ciberseguridad
- En cuestiones legales sobre ciberseguridad
- Información de estado de seguridad.

5. Componentes del SOC

Los diferentes componentes constitutivos del SOC de acuerdo al marco de referencia PPTGC, antes expuesto, se comentan a continuación.

5.1. Personal

El equipo del SOC tendrá personas para la realización de sus funciones con conocimientos escalonados de acuerdo a los roles que es indican en la figura:

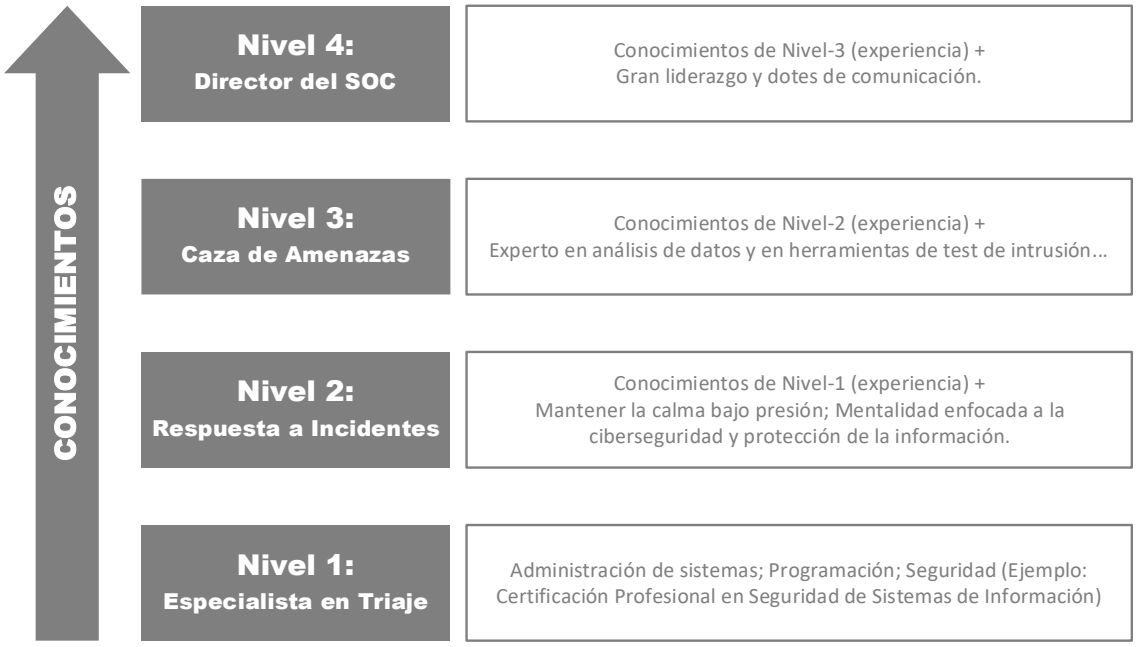

Ilustración 4. Conocimientos de los diferentes roles del SOC

Además de estos roles básicos, también encontramos en los SOCs otros como:

5.1.1. Roles de gestión

En un SOC, el rol de gestión más alto jerárquicamente es la autoridad ejecutiva correspondiente (en una compañía puedes ser el CISO[10]), responsable de las estrategias y objetivos de las operaciones de seguridad. En el caso del G-SOC esta función puede estar en las entidades, dada la autonomía funcional.

[10] Director de seguridad de la información (en inglés, *Chief information security officer*).

El rol ejecutivo más obvio es el **director del G-SOC** que, obviamente, gestiona el SOC.

También es habitual en estos centros la figura del **coordinador de respuesta a incidentes**.

5.1.2. Roles técnicos

Expertos técnicos en **áreas de conocimiento específico** (malware, Threat Hunters, Forensic Specialists, expertos en valoración de vulnerabilidades…) o expertos en **herramientas/aplicaciones concretas** del SOC de gran complicación (NG-FW, IPSs, DLP/IRM, SIEM…).

5.1.3. Roles consultivos

Como, por ejemplo, el **arquitecto de seguridad** (evalúa y diseña las soluciones de seguridad de la organización en las infraestructuras) o el **consultor de ciberseguridad**, para temas especialmente complejos.

5.1.4. Personal externo

En todos los niveles del SOC puede haber **personal externo para apoyo** a tareas concretas o proyectos coyunturales. También puede haber **personal de proveedores** dando servicios de asesoramiento en productos o soluciones.

Como en cualquier otro ámbito laboral, aspectos como el reclutamiento, la retención, la formación continua y la colaboración y la comunicación son básicos en el rendimiento y eficacia del trabajo que redunda en la calidad del SOC.

5.2. Procesos

Dado que la finalidad del SOC es responder o prepararse para incidentes, los procesos esenciales pueden considerarse desde el punto de vista del Ciclo de Vida de Respuesta a Incidentes de Seguridad Informática. Acorde con el NIST[11], comprende los cuatro pasos "preparación", "detección y análisis", "contención, erradicación y recuperación" y "actividad posterior al incidente".

Ilustración 5. El ciclo de vida de la respuesta a incidentes de seguridad del NIST.

5.2.1. Preparación

Las actividades para prepararse ante los incidentes conllevan **compilar la lista de activos de TI**, como redes, servidores y terminales, identificando su importancia y cuáles son críticos o contienen datos confidenciales. Después, se debe **configurar la monitorización** y **disponer de una línea base de actividad normal** con la que **comparar**. Hay que determinar qué **tipos de eventos de seguridad deben investigarse** y crear los **pasos de respuesta detallados** para los tipos de incidentes más comunes.

El proceso de recopilación de datos, es un buen ejemplo de proceso para la fase de preparación ante incidentes que se deberá realizar en un SOC eficiente. Se muestra esquemáticamente en la siguiente ilustración (el orden de los diferentes pasos del proceso puede variar):

[11] El Instituto Nacional de Estándares y Tecnología (NIST) es una agencia operada por el Departamento de Comercio de los Estados Unidos que proporciona estándares y recomendaciones para muchos sectores tecnológicos.

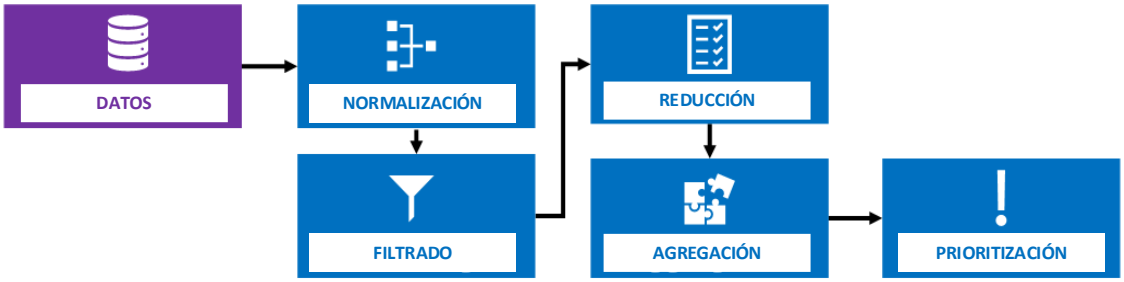

Ilustración 6. El proceso de recopilación de datos.

5.2.2. Detección y analisis

Los pasos generales constitutivos de este proceso son:

1. Detección

   La detección se lleva a cabo por **procedimientos automáticos** complementados con la **experiencia y conocimientos del personal del SOC**.

   Conlleva recopilar datos de los sistemas de TI, herramientas de seguridad, cotejando información disponible públicamente y con la asistencia de personas dentro y fuera de la organización, para con todo ellos identificar precursores (signos de que un incidente puede ocurrir en el futuro) e indicadores (datos que muestran que un ataque ha ocurrido o está ocurriendo).

2. Análisis

   Implica **identificar una actividad normal** o de referencia para los sistemas afectados, **correlacionar eventos relacionados** y **ver si se desvían del comportamiento normal y cómo**.

3. Priorización de alertas (Triaje)

   Busca que los incidentes más graves se traten con **prioridad** y que los incidentes se reparten de acuerdo con los recursos disponibles para su procesamiento.

5.2.3. Contención, erradicación y recuperación

La **contención** persigue detener el ataque antes de que desborde los recursos o cause daños. Ha de buscar el compromiso entre los daños, el mantenimiento de servicios críticos y valoración de la solución (provisional/permanente, dificultad de implementación, costes, riesgos…).

En la etapa de **erradicación y recuperación**, una vez que el incidente se ha contenido con éxito, se debe actuar para eliminar todos los elementos del incidente del entorno.

Erradicada la amenaza, hay que **restauraar los sistemas y recuperar las operaciones** normales lo antes posible. Finalmente, habrá que tomar medidas para garantizar que el ataque no se repita.

La siguiente figura muestra el flujo y acciones del proceso de Contención, erradicación y recuperación:

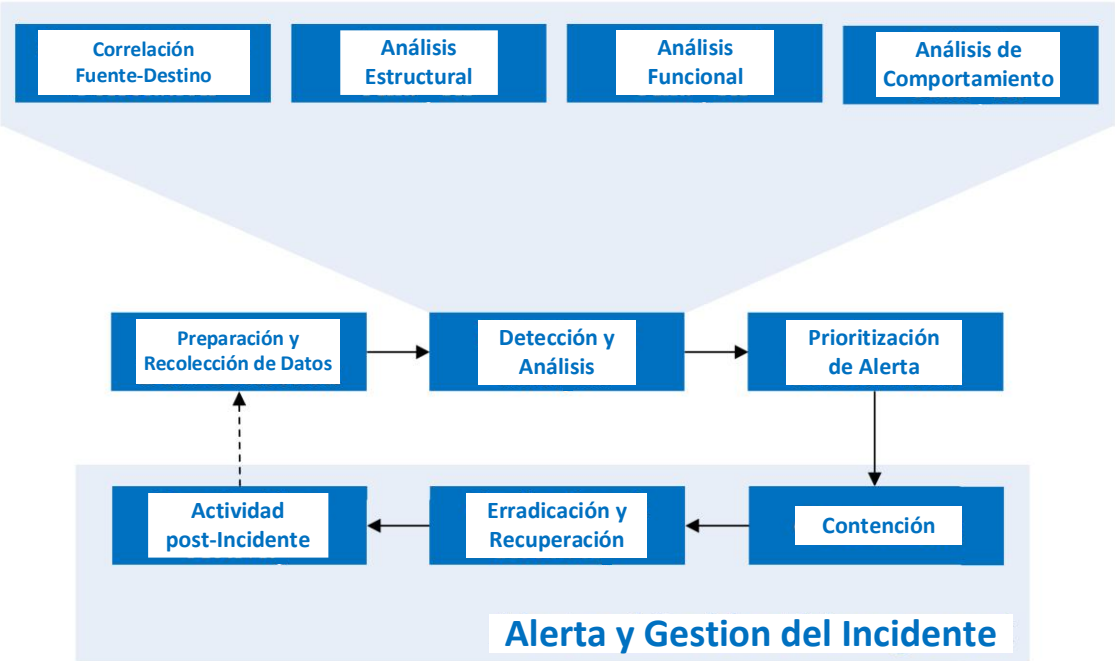

Ilustración 7. El proceso de análisis, detección y gestión de incidentes del SOC.

5.2.4. Actividad post-Incidente

Aprender de los incidentes para mejorar los procesos, es clave. Se ha de **revisar, analizar y documentar cada incidente**, utilizando los hallazgos para **mejorar los procesos**, ajustar las políticas, planes y procedimientos de respuesta a incidentes.

5.3. Tecnología

Se consideran en Tecnología las diferentes herramientas/aplicaciones utilizadas en los SOCs, Estas son muy numerosas y variadas, por lo que nos limitamos aquí a enumerar algunas específicas de ciberseguridad.

Como ejemplo de SW de seguridad citaremos:

- Sistemas SIEM
- Sistemas de detección/prevención de intrusos (IDS/IPS, NIDS)
- Cortafuegos (Firewalls)
- Software antivirus (EDR, EPP)
- Escáneres de vulnerabilidad
- Gestión de identidad y acceso (NAC)
- Cortafuegos de aplicaciones WEB (WAF)
- Protección contra pérdidas de datos (IRM / DLP)
- Etc.

En el documento que presenta **la propuesta del G-SOC AR se concretan herramientas aconsejadas**, de acuerdo a las conversaciones mantenidas en las reuniones con el CERT AR.

5.4. Gobernanza y cumplimiento

Muchos de los procesos del SOC están gobernados por las "buenas prácticas" establecidas, aunque también **requisitos de cumplimiento de normativas** rigen algunos procesos. El SOC es responsable de auditar regularmente sus sistemas para garantizar el cumplimiento de dichas regulaciones, que pueden ser emitidas por su organización, por su industria o por los órganos de gobierno.

Ejemplos de estas regulaciones en diferentes sectores incluyen HIPAA[12] (Sanidad), PCI DSS[13] (tarjetas de crédito) y GDPR[14] (protección de datos). Ajustarse a las normativas no solo ayuda a proteger datos sensibles confiados a la entidad o empresa, también **protegerá a la organización de daños a la reputación y desafíos legales que resulten de una infracción**.

Desde el SOC pueden desarrollarse programas o scripts que comprueben el cumplimiento, iniciando sesiones de forma remota en un sistema, recopilando su configuración y luego analizándola contra un modelo de referencia (herramientas comerciales como *Qualys, Nessus, Nexpose* y otras) incluyen un módulo a tal fin)

Automatizar el proceso de cumplimiento del sistema es clave en cualquier operación de seguridad exitosa.

[12] Ley de Responsabilidad y Portabilidad del Seguro de Salud (USA)
[13] El estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) es un estándar de seguridad de la información para organizaciones que manejan tarjetas de crédito de marca de los principales esquemas de tarjetas.
[14] Reglamento General de Protección de Datos (Unión Europea)

6. Retos

A la hora de diseñar e implantar un SOC y en su desarrollo y mejora nos enfrentaremos a una serie de **desafíos** no sencillos que habrá que **gestionar y superar**. Se señalan a continuación los más importantes, organizados en relación a las cuatro dimensiones del marco de referencia PPTGC, mediante la figura siguiente:

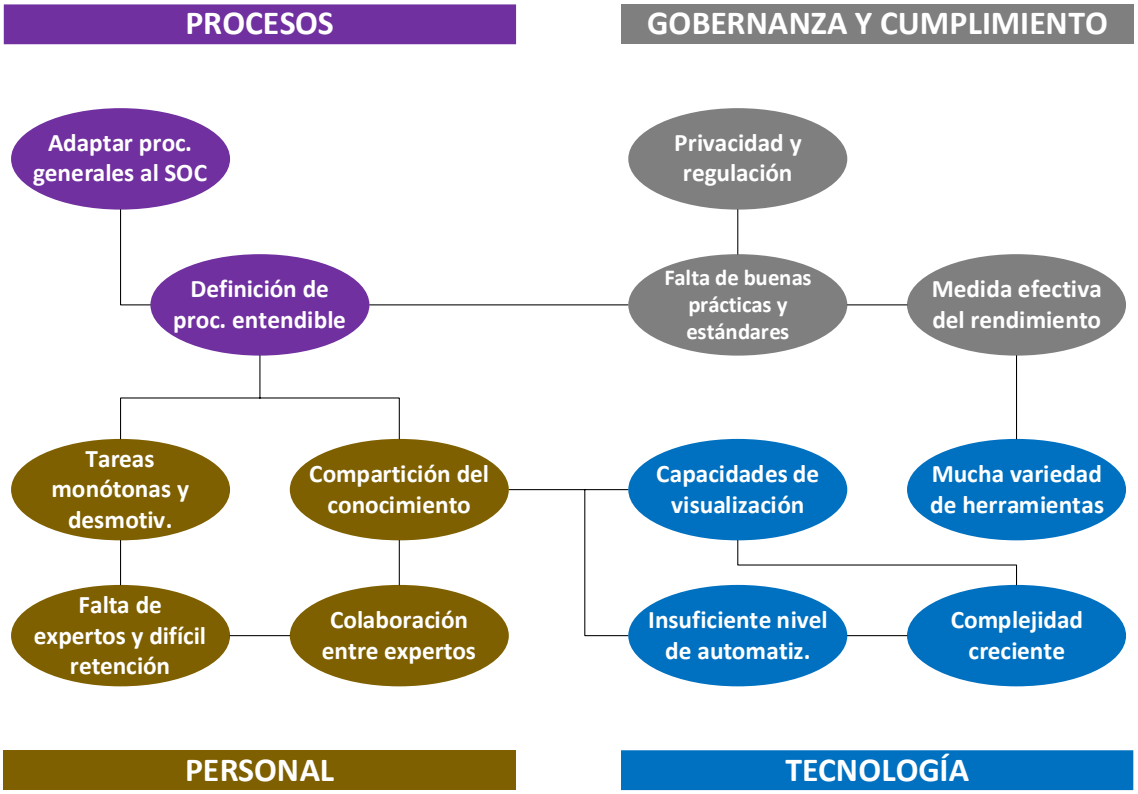

Ilustración 8. Retos para el desarrollo y mejora de los SOC.

7. Status global de ciberseguridad en la APN

Los aspectos que se han considerado más relevantes en cuanto al estado de la ciberseguridad en la APN en Argentina, de acuerdo a los datos revisados, son los siguientes:

- En lo relativo a la ciberseguridad **las entidades de la APN son autónomas** en su funcionamiento, lo que dificulta las sinergias que podrían aprovecharse con una colaboración más estrecha.

- Cada organismo de la APN, en la situación vigente, debe procurarse y gestionar sus propios servicios de ciberseguridad. Para conseguirlo cuenta **sólo con su propio personal, no siempre suficientemente experto y especializado, y los recursos propios del organismo**, lo que supone un gran esfuerzo, tanto económico como organizativo.

- Con el actual panorama en el mundo digital y en un escenario de esfuerzos individuales de los organismos, el incremento cada vez más rápido en la **cantidad y complejidad de las ciberamenazas** sobre las tecnologías de la información, **las capacidades de prevención, protección, detección y respuesta de las entidades de la APN resultan casi siempre insuficientes y son costosas y difíciles de aumentar**.

- Las entidades de la APN no son homogéneas y tienen **características muy variadas** en aspectos como:

    - **Volumetrías** de usuarios, de dispositivos, de sedes, de redes, de tráfico de red, etc.

    - **Tecnologías** utilizadas, marcas y modelos de equipos y dispositivos de red, sistemas operativos, etc.

    - **Servicios y herramientas de ciberseguridad** como cortafuegos, antivirus, IDS/IPS, equipos de conexión a Internet, proxies, NAT, etc.

  Una taxonomía y caracterización de las entidades no resultaría demasiado útil y no ha estado disponible en este análisis.

- LA APN a día de hoy **no tiene una red troncal que conecte a las entidades** que la forman. En general, **cada entidad cuenta con una conexión a Internet**, a través de la que se ofrecen servicios al ciudadano (Portales WEB, administración electrónica) y, a su vez, se obtienen servicios (correo electrónico, navegación, consultas…). También es por donde llegan la mayoría de los ataques de ciberseguridad.

Esta falta de red troncal **obliga a utilizar Internet para el despliegue de un G-SOC**[15] capaz de monitorizar eventos de seguridad en las entidades.

- Actualmente, el organismo con la misión de apoyo en asuntos de ciberseguridad a los organismos de la APN es el **CERT AR**[16], creado[17] en el ámbito de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD por Disposición 1/2021[18]. Sus funciones aparecen enumeradas en su página WEB[19] y están dirigidas, fundamentalmente, a la ayuda y asistencia en incidencias graves de ciberseguridad: "*Contribuir a **incrementar la capacidad de prevención, alerta, detección y recuperación ante incidentes de seguridad informática** que puedan afectar activos de información críticos del país*".

  Su asistencia se ofrece **bajo demanda** del organismo que reporta el incidente y sus **funciones son consultivas** y de asesoría (la entidad puede o no seguir las pautas y consejos del CERT, de acuerdo a su propio criterio). **Los medios con los que cuenta el CERT son limitados,** tanto en lo material (aplicaciones/herramientas, acceso a la información, etc.) como de personal (número de técnicos, capacitación etc.).

  Así, **el G-SOC AR puede verse como la evolución natural del CERT AR**, un paso adelante en las capacidades y medios disponibles para contribuir más eficazmente en las funciones que ya tiene encomendadas.

- La infraestructura de red WAN[20] en la que se basan las comunicaciones de las entidades de la APN la provee **ARSAT**, principal empresa de telecomunicaciones argentina que, además de las facilidades de transporte (**líneas de transmisión**, circuitos), también aloja en su Centro Nacional de Datos a muchos de los proveedores de servicios más habituales (proveedores de Internet ISP, VISP; de acceso, de correo electrónico, de hosting etc.). ARSAT dispone de bastantes recursos humanos y materiales para la monitorización y gestión de su red, lo que hace que el CERT AR busque en ocasiones apoyo en el NOC[21] de ARSAT, aunque la función del NOC no sea específicamente la ciberseguridad.

- En cuanto a incidentes de ciberseguridad, en el ***Informe anual de incidentes de seguridad informática registrados en el 2020*** y **en el 2021**[22], se analizan los incidentes reportados en los que ha colaborado el **CERT**. Su número es reducido, 226 en 2020 y 591 en 2021, debido mayormente a que las entidades de **la APN sólo reportan los casos que quieren**: el marco normativo no les obliga a compartir información con el CERT.

[15] Como se indica en el documento de diseño del G-SOC propuesto, esta carencia de red troncal no es un obstáculo insalvable: pueden usarse sondas en el organismo para reportar eventos, que se comuniquen con el G-SOC usando "túneles IP cifrados".
[16] https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar
[17] https://blog.segu-info.com.ar/2021/02/argentina-crea-el-nuevo-certar.html
[18] https://www.boletinoficial.gob.ar/detalleAviso/primera/241077/20210222
[19] https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/misiones-y-funciones-del
[20] WAN (Wide Area Network), "red de área amplia" que interconecta las redes locales de una organización, usando generalmente servicios de un operador de telecomunicaciones o Internet.
[21] NOC es el centro de operación de red (Network Operation Center)
[22] https://www.argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f__0.pdf

- En el informe del CERT se analizan y clasifican los incidentes, tanto por sectores, como por tipo, así como por su gravedad. Aunque el **incremento de 2020 a 2021 es notable**, de 226 a 591 respectivamente, no deja de ser **extremadamente bajo**. Esto se debe a lo ya apuntado, las entidades no tienen ninguna obligación de reportarlos, pero también a la **falta de medios materiales y de personal**.

- Otro aspecto preocupante es el relativo a la **gravedad en los incidentes y el tiempo de resolución**. Según datos de la SIT[23], el 81,7% de los incidentes procesados durante 2021 fueron de severidad alta o crítica, que tienen un costo 100 veces mayor que los de severidad baja.

[23] Secretaría de Innovación Tecnológica

8. Justificación para el despliegue de un G-SOC

Los **ataques de seguridad** son cada vez más complejos y exhiben capacidades **cada vez más sofisticadas**. Por lo tanto, abordar la complejidad y sofisticación de tales ataques debe incluir no solo invertir en medidas preventivas, sino también el **desarrollo de capacidades de monitoreo inteligente e integradas** incorporadas en un programa de respuesta a incidentes.

La situación descrita en el punto anterior, claramente apunta a la necesidad de reforzamiento de las capacidades de prevención, protección, detección y respuesta de las entidades de la APN. La mejor manera de abordar este objetivo es mediante la **creación de un G-SOC** que utilice y aproveche los conocimientos, las tecnologías y herramientas que hoy en día se desarrollan en toda la comunidad digital para defender los activos informáticos presentes en todos los sectores de la sociedad y dar **respuesta a los retos planteados**.

Un G-SOC al servicio de las entidades de la APN que permitirá **monitorear, en tiempo real, ataques y amenaza a las ICI**. Sería la forma natural de **potenciar el actual CERT** (Centro de Respuesta a Incidentes de Ciberseguridad Nacional), actualmente sin las capacidades para gestionar las respuestas a incidentes, complementándolo **con otras funciones adicionales** como asesoría de ciberseguridad o sumando herramientas (por ejemplo, un mecanismo seguro y confidencial para intercambiar información con el ecosistema nacional relativo a ataques e incidentes).

Se citan a continuación, problemas y desafío identificados por el IADB

- El **alto costo de los incidentes de ciberseguridad** para el Estado y la ciudadanía. Este es un problema capital y creciente (los ataques/incidentes cada vez revisten mayor gravedad, como ilustran casos recientes[24])
- **Baja cobertura de la SIT para identificar y proteger ICI**.
- **Baja eficiencia en la gestión de incidentes cibernéticos** (detección, respuesta y recuperación).
- **Escasez de personal capacitado** en ciberseguridad.

Los objetivos señalados para paliar los problemas enumerados, contribuyendo con ello a la **reducción de los costos** por incidentes de ciberseguridad para el Estado y la ciudadanía, incluyen **mejorar la eficienc**ia en la gestión de **incidentes** cibernéticos y en la gestión **de la ciberseguridad en general y de los ICI** en particular. Un G-SOC eficaz, bien gestionado e integrado con el CERT AR al servicio de la APN, es seguramente, la mejor forma de conseguirlo.

[24] En 2020 la Oficina Nacional de Migraciones sufrió un ciberataque que afectó sus servicios digitales impidiendo ingresos y egresos de personas al país.
En 2021 el Registro Nacional de las Personas sufrió un el robo de información sensible de millones de argentinos.

ANEXO: Lista de acrónimos en el documento

Acrónimo	Significado
ALC	America Latina y el Caribe
APN	Administración Pública Nacional
BA-CSIRT	Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires
BID	Banco Interamericano de Desarrollo (tb. IADB en inglés)
CC	Comité de Ciberseguridad
CERT	Computer Emergency Response Team (en español, Centro Nacional de Respuesta a Incidentes)
CERT.ar	Equipo de Respuesta ante Emergencias Informáticas nacional de Argentina (Computer Emergency Response Team)
CERT/CC	CERT Coordination Center
CIIP	Protección de las Infraestructuras Críticas de Información
CISO	Director de seguridad de la información (en inglés, Chief information security officer)
CMM	Capability Maturity Model
CMU	Universidad Carnegie Mellon
CSIRT	CyberSecurity Incident Response Team (en español, Equipo de Respuesta a Incidentes de Ciberseguridad)
DLP	Data Loss Prevention (en español Prevención de Pérdida de Información);
DNCP	Dirección Nacional de Contrataciones Públicas
EDR / EPP	Software antivirus (Endpoint Detection Response / Endpoint protection platform)
ENC	Estrategia Nacional de Ciberseguridad
GCSCC	Centro Global de Capacidad en Seguridad Cibernética
GDE	Gestión Documental Electrónica (catalogado como un ICI)
G-SOC (o GSOC)	Goverment SOC (en español SOC gubernamental)
IADB	Inter-American Development Bank (tb. BID en español)
ICI	Infraestructuras Criticas de Información
ICIC	Infraestructura de Información Crítica y Ciberseguridad
ICS	Innovation for Citizen Services
IDS	Sistema de detección de intrusos (en inglés Intrusion Detection System))
IFD	Institutions for Development
INAP	Instituto Nacional de la Administración Pública
IPS	Sistema de prevención de intrusos (en inglés Intrusion Prevention System)
IRM	Information Rights Management (en español Gestión de los derechos de la Información)
ISOC	Information Security Operations Center
JGM	Jefatura de Gabinete de Ministros
NAC	Gestión de identidad y acceso
NAT	Network Address Translation
NG-FW	Cortafuegos de nueva generación
NIST	Instituto Nacional de Estándares y Tecnología (agencia de USA)

Acrónimo	Significado
NOC	Network Operations Center
PPTGC	Personas, Procesos y Tecnología, Gobernanza y Cumplimiento
SIEM	Gestión de información y eventos de seguridad
SIT	Secretaría de Innovación Tecnológica
SOC	Security Operation Center (en español, Centro de Operaciones de Ciberseguridad)
SW	Software
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y Comunicaciones
WAF	Cortafuegos de aplicaciones WEB