Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Electrónica y Eléctrica
Escuela Profesional de Ingeniería Electrónica

Implementación de servicio de centro de operaciones de ciberseguridad (CYBERSOC) con plataformas opensource a entidad financiera

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Willy Franz VASQUEZ BARZOLA

ASESOR

Mg. Luis Ernesto CRUZADO MONTAÑEZ

Lima, Perú

2023

Referencia bibliográfica

Vasquez, W. (2023). *Implementación de servicio de centro de operaciones de ciberseguridad (CYBERSOC) con plataformas opensource a entidad financiera*. [Trabajo de Suficiencia Profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Willy Franz Vasquez Barzola
Tipo de documento de identidad	DNI
Número de documento de identidad	45896191
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Luis Ernesto Cruzado Montañez
Tipo de documento de identidad	DNI
Número de documento de identidad	32920395
URL de ORCID	https://orcid.org/0000-0002-1056-8973
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Jose Vidal Huarcaya
Tipo de documento	DNI
Número de documento de identidad	09450859
Miembro del jurado 1	
Nombres y apellidos	Edmundo Picon Llanos
Tipo de documento	DNI
Número de documento de identidad	07564597
Miembro del jurado 2	
Nombres y apellidos	Angel Orlando Sumoso Huaman
Tipo de documento	DNI
Número de documento de identidad	06842634
Datos de investigación	
Línea de investigación	E.3.3.5 Métricas de la información y evaluación de la producción científica
Grupo de investigación	No Aplica

Agencia de financiamiento	No Aplica
Ubicación geográfica de la investigación	Edificio: Av. Juan de Arona 755, Piso 10, Oficina 105 País: Perú Departamento: Lima Provincia: Lima Distrito: San Isidro Latitud: -12.0961947 Longitud: -77.0286332
Año o rango de años en que se realizó la investigación	Noviembre 2020 - diciembre 2021
URL de disciplinas OCDE	Ciencias de la Información https://purl.org/pe-repo/ocde/ford#5.08.02 Ciencias de la computación https://purl.org/pe-repo/ocde/ford#1.02.01

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERIA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL Nº 059/FIEE-EPIE/2023

Los suscritos Miembros del Jurado, nombrados por la Comisión Ejecutiva del Programa de Perfeccionamiento Profesional de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha, bajo La Presidencia del **ING. JOSE VIDAL HUARCAYA,** integrado por el **ING. EDMUNDO PICON LLANOS,** el **ING. ANGEL ORLANDO SUMOSO HUAMAN** y Miembro Asesor el **MG. LUIS ERNESTO CRUZADO MONTAÑEZ.**

Después de escuchar la Sustentación de Trabajo de Suficiencia Profesional del **Bach. WILLY FRANZ VASQUEZ BARZOLA** con código **N° 06190121** que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulado **IMPLEMENTACIÓN DE SERVICIO DE CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC) CON PLATAFORMAS OPENSOURCE A ENTIDAD FINANCIERA.**

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió aprobar otorgándole el calificativo de **diecisiete (17).**

Ciudad Universitaria, 13 de mayo del 2023

ING. JOSE VIDAL HUARCAYA
Presidente de Jurado

ING. EDMUNDO PICON LLANOS
Miembro Jurado

ING. ANGEL SUMOSO HUAMAN
Miembro de Jurado

MG. LUIS ERNESTO CRUZADO MONTAÑEZ
Miembro Asesor

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
ESCUELA PROFESIONAL DE INGENIERIA ELECTRONICA

INFORME DE ORIGINALIDAD

1. Facultad de Ingeniería Electrónica y Eléctrica.
2. Escuela Profesional de Ingeniería Electrónica.
3. Emisor del Informe el presidente de la Comisión Ejecutiva del Pro0grama de Perfeccionamiento Profesional.
4. Operador del programa informático de similitudes: Edy Alberto Román Ccorahua.
5. Documento evaluado: Trabajo de Suficiencia Profesional para título de (pregrado) **IMPLEMENTACIÓN DE SERVICIO DE CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC) CON PLATAFORMAS OPENSOURCE A ENTIDAD FINANCIERA**
6. Autor de la tesis: **WILLY FRANZ VASQUEZ BARZOLA**
   Fecha de aplicación de recepción del documento: 13-04-2023
7. Fecha de aplicación del programa informático de similitudes: 13-04-2023
8. Software utilizado: Turnitin.
9. Configuración del programa detector de similitudes:
   - Excluye citas.
   - Excluye bibliografía.
   - Excluye cadenas menores de 40 palabras
10. Porcentaje de similitudes según programa detector: Nueve por ciento – 9%
11. Fuentes originales de las similitudes encontradas.

1. hdl.handle.net	4% Fuente de Internet
2. ciberseguridad.neosecure.com	1% Fuente de Internet
3. www.oas.org	1% Fuente de Internet
4. securitcrs.wordpress.com	1% Fuente de Internet
5. assets.ey.com	1% Fuente de Internet
6. dspace.ups.edu.ec	<1% Fuente de Internet
7. repository.uniminuto.edu.8080	<1% Fuente de Internet
8. Submitted to Universidad Nacional Abierta y a Distancia, UNAD.UNAD	<1% Fuente de Internet
9. Usecim.net	<1% Fuente de Internet

12. Observaciones: Ninguna.
13. Calificación de originalidad.
    - Documento cumple criterios de originalidad, sin observaciones.
14. Fecha del informe: 29 de mayo del 2023.

Atentamente,

Mg. Edy Alberto Román Ccorahua
Presidente de la Comisión Ejecutiva del Programa de Perfeccionamiento Profesional

RESUMEN

El presente informe tiene como objetivo mostrar la estructura de implementación de un servicio CyberSOC, el cual incluye 5 subservicios que en conjunto permiten cubrir el entorno de ciberseguridad para una entidad financiera y reducir así las brechas de ciberseguridad existentes a las que se exponen.

Los 5 subservicios consisten en:

- Monitoreo de infraestructura de TI.
- Gestión de vulnerabilidades infraestructura de TI.
- Correlación avanzada de logs de seguridad.
- Procedimiento de respuesta ante incidentes de ciberseguridad.
- Procedimiento de análisis forense.

La solución será implementada en un ambiente cloud el cual se integrará con la infraestructura TI de la entidad, se mostrará los elementos y tecnologías empleadas para llevar a cabo la configuración de notificaciones necesarios de acuerdo con los requerimientos solicitados.

En los resultados se reflejará la cantidad de vulnerabilidades, cantidad de alertas clasificados por severidad, la cuales están sujetas a Acuerdo de Niveles de Servicio (SLA), los mismos que posteriormente permitirán elaborar un plan de corrección y seguimiento.

Finalmente, esta solución permite incentivar a las pequeñas empresas a apostar en una inversión con plataformas open source para mejorar el indicador de madurez en ciberseguridad y así reducir la probabilidad de impacto en el negocio tales como pérdidas económicas, reputacionales entre otros.

Palabras clave:

Cyber SOC, open source, ciberseguridad, vulnerabilidad y Graylog

ABSTRACT

The objective of this report is to show the implementation structure of a CyberSOC service, which includes 5 subservices that together cover the cybersecurity environment for a financial institution and thus reduce the existing cybersecurity gaps to which they are exposed.

The 5 subservices consist of:

- Monitoring of IT infrastructure.
- Management of IT infrastructure vulnerabilities.
- Advanced correlation of security logs.
- Response procedure for cybersecurity incidents.
- Forensic analysis procedure.

The solution will be implemented in a cloud environment which will be integrated with the entity's IT infrastructure, the elements and technologies used to carry out the configuration of necessary notifications will be shown according to the requested requirements.

The results will reflect the number of vulnerabilities, the number of alerts classified by severity, which are subject to a Service Level Agreement (SLA), which will later allow the preparation of a correction and follow-up plan.

Finally, this solution allows small companies to bet on an investment with open-source platforms to improve the cybersecurity maturity indicator and thus reduce the probability of impact on the business such as economic and reputational losses, among others.

Keywords:

Cyber SOC, open source, cybersecurity, vulnerability, and Graylog

INDICE

LISTADO DE TABLAS

LISTADO DE FIGURAS

CAPITULO I
INTRODUCCIÓN

Hoy en día la ciberseguridad toma relevancia debido a que las empresas buscan proteger su infraestructura y su información a través del uso de mecanismos informáticos de piratas ya que los métodos convencionales de seguridad no son los adecuados para enfrentar amenazas que varían desde ataques simples hasta ataques avanzados que se presentan en internet; la OEA a raíz de los eventos desencadenados por la pandemia del COVID 19 publicó un reporte en el que evidencia que la región de América Latina y en especial el Perú no se encuentra preparado para defenderse de ataques cibernéticos, por lo que las empresas buscan a menudo proveedores y especialistas en ciberseguridad que tengan conocimientos del uso de mecanismos informáticos, uno de estos mecanismos es los Centros de Operaciones de Ciberseguridad (CYBERSOC) con plataformas OpenSource que involucra el uso de temas estratégicos y operativos que se relacionan con los temas de seguridad informática, el equipo constituido en esta unidad realiza labores de monitoreo, aseguramiento y defensa de los activos de la información mediante el uso de equipos tecnológicos; en el presente informe se analiza su comportamiento y su efectividad a causa de su implementación en una entidad financiera, en el informe se dan a conocer sus mecanismos de funcionamiento, requisitos para su implementación y sus resultados.

CAPITULO II
INFORMACION DEL LUGAR DONDE SE DESARROLLO LA ACTIVIDAD

2.1 Institución donde se desarrolló la actividad

ROYAL ITC S.A.C

2.2 Periodo de duración de la actividad

El periodo de duración de la actividad fue desde 18/11/2020 hasta 31/12/2021

2.3 Finalidad y objetivo de la entidad

Empresa dedicada a la consultoría y mejora de procesos, su propuesta de valor consiste en soluciones simples y servicios efectivos que impulsan resultados exitosos. Brinda servicios de CyberSOC (CyberSecurity Operation Center) a entidades financieras.

2.4 Visión de la entidad

Tener posición de empresa líder en el mercado brindando soluciones de ingeniería y tecnología de manera eficiente y simple, generando valor en las organizaciones del medio; además ser el socio principal que brinda asistencia en la construcción de relaciones de confianza a largo plazo.

2.5 Misión de la entidad

Contribuir conjuntamente con sus clientes en el logro de sus objetivos y acompañarlos en el camino al liderazgo en el sector en el que se desenvuelvan, en un entorno global de cambio continuo a través de soluciones que agreguen valor y reconocimiento, con ética, aporte de especialización y experiencia de nuestros recursos.

2.6 Razón social de la entidad

ROYAL ITC S.A.C perteneciente a la corporación ROYAL SUN CORPORATION S.A.C.

2.7 Correo electrónico del profesional a cargo

Erle Paredes Ruiz - erle.paredes@royalcor.com

CAPÍTULO III
DECRIPCIÓN DE LA ACTIVIDAD

3.1 Finalidad y Objetivos de la actividad

3.1.1 Finalidad

Disminuir el impacto y probabilidad de los riesgos cibernéticos y establecer procedimientos mínimos necesarios en la entidad con la implementación de un Centro de Operaciones de Ciberseguridad (CyberSOC) usando plataformas opensource.

3.1.2 Objetivos

3.2.1.1 Objetivo general

Implementar servicio de centro de operaciones de ciberseguridad (CyberSoC) con plataformas opensource a una entidad financiera, que permita el monitoreo, detección, análisis, prevención y seguimiento de eventos e incidentes de ciberseguridad en los equipos e instalaciones de la entidad financiera a través del uso de herramientas tecnológicas.

3.2.1.2 Objetivos Específicos.

- Diseñar la topología necesaria para la implementación del Centro de Operaciones de Ciberseguridad.
- Diseñar e implementar la Plataforma e gestión de alertas de

servidores
- Diseñar e implementar la Plataforma de alertas de seguridad
- Establecer procedimientos para la respuesta ante incidencias de seguridad, reportes, reportes de inteligencia de amenazas, análisis forense y gestión de vulnerabilidades.

3.2 Problemática

3.2.1 Problema principal

¿Es posible Implementar un servicio de Centro de Operaciones de Ciberseguridad (CyberSoC) con plataformas opensource a una entidad financiera?

3.2.2 Problemas Específicos

- ¿Cómo Diseñar la topología necesaria para la implementación del Centro de Operaciones de Ciberseguridad?
- ¿Cómo diseñar e implementar la Plataforma e gestión de alertas de servidores?
- ¿Cómo diseñar e implementar la Plataforma de alertas de seguridad?
- ¿Cómo establecer procedimientos para la respuesta ante incidencias de seguridad, reportes, reportes de inteligencia de amenazas, análisis forense y gestión de vulnerabilidades?

3.3 Metodología

3.3.1 Antecedentes de la investigación

(Ormachea, 2020) menciona que los avances tecnológicos son un desafío para la seguridad y la defensa de los países, es por ello que los

principales responsables de las políticas deben tener en cuenta dicha problemática y asumir la responsabilidad de la seguridad y la defensa de los países conteniendo las amenazas que provienen del ciberespacio en el que la vida de las naciones transcurre de manera diferente al plano físico, pero que es capaz de alterar la realidad de dicho plano; el autor resalta que a nivel global existe dependencia de los estados con los sistemas de información constituyendo la gran fortaleza de los mismos y a la vez su gran debilidad, más a pesar de ello son más personas las que se encuentran interconectadas, siendo una tendencia imparable, algo que requiere la gestión de riesgos derivados de estos; el ciberespacio recibe amenazas variadas, pero se observa que son en mayor número los ataques de grupos organizados que por delincuentes individuales y los ataques se orientan más contra los organismos fundamentales de cada nación, las libertades públicas y servicios en los que basa su marcha la sociedad. El Perú es un país en el que existe poca conciencia en aspectos de protección y riesgos en términos de materia de seguridad informática, además de ello es un país en el que la legislación es pequeña para temas de seguridad de la información y la seguridad informática, mucho más en temas de ciberdefensa y ciberseguridad.

La revista Kaspersky Lab, hizo una encuesta a finales del 2016 que se aplicó a más de 4000 empresas en 25 países y con los resultados se pudo observar que el 38% de los encuestados mencionaron experimentó problemas con virus y softwares maliciosos y con ellos una disminución notable en su productividad, también se pudo observar que el 21% había sufrido pérdidas de datos por filtraciones debido a ataques dirigidos, el 40% de los encuestados sufrían de preocupación ante estas amenaza, respecto a las empresas se pudo observar que el 17% de estas había sido víctima de ataques de DDoS, además es 42% de los encuestados experimentaron ataques de phishing y fueron en grandes empresas, el 26% de los eventos de ataque que violaron la seguridad no se detectaron por varias semanas o más y las que se detectaron solo quedaron al descubierto mas no se tomaron las medidas respectivas y el impacto financiero ocasionado promedio por la vulneración de datos fue de USD 891000 de manera global y para una empresa el perjuicio estuvo dentro de los valores de USD 393000 y USD 1100000 dependiendo de la gravedad del problema de seguridad (Kapersky Lab , 2017).

De acuerdo con la revista Execution de seguridad informática en su volumen XIII que se lanzó en el año 2022, los ciberataques se han vuelto un problema mucho más agravado a causa de la pandemia del COVID 19, ya que esta ha promovido el desarrollo de una adopción tecnológica sin igual que incrementa los riesgos; además el autor resalta que los ciberataques son por lo menos de 10 tipos y de los más conocidos son: Denial of service (DoS), Phising, Pasword Cracking, entre otros y el Perú no es ajeno a este tipo de ataques; según un reporte de Fortinet en el 2021 Latinoamérica fue víctima de más de 91000 millones de ataques cibernéticos y los países que más fueron atacados fueron: México (60.8 mil millones), Brasil (16.2 mil millones), Perú (4.7 mil millones) y Colombia (3.7 mil millones), además de ello los resultados de la encuesta realizada de EY a 411 CEO's, CIO's y otros ejecutivos que se encargaban de la ciberseguridad para conocer las acciones tomadas en favor de la ciberseguridad en el futuro, a lo que ellos respondieron a la pregunta ¿Cuáles de las acciones prevé que se llevara a cabo en su organización en los próximos 12 meses?, la mayoría respondió que serían las inversiones significativas en datos y tecnología, es así que se evidenció que en el 2021 muchas de las empresas se vieron con la obligación de adaptarse a un perfil de riesgo cibernético diferente; también se reportaron datos que engloban a los gastos en ciberseguridad a nivel global, Latinoamérica y Perú que fueron 22%, 14% y 11% respectivamente (EY, 2022).

3.3.2 Bases teóricas

3.3.2.1. Seguridad informática

(Avenía, 2017) define a la seguridad informática tomando en cuenta los términos de su procedencia que son: el término latín *securitas* que se centra en la propiedad de seguro, una cosa es segura si es algo fuerte, cierta e indudable; en el caso de equipos informáticos, de acuerdo a (Roa, 2013) engloba a las aplicaciones que se ejecutan en estos en contra de amenazas como:

- **Desastres Naturales:** Cuando existe la posibilidad de eventos como incendios, inundaciones, entre otros; ante estos se tiene en cuenta la hora de emplazamiento del centro de proceso de datos (CPD) y en ocasiones se cuenta con un segundo CPD para que la actividad no pare.

- **Robos:** La información que guardan los equipos son de vital importancia tanto para las personas y organizaciones, por lo que se debe proteger el acceso a estas mediante medidas de seguridad.

- **Fallas de suministro:** Los ordenadores funcionan gracias a la corriente eléctrica y se encuentran en constante contacto con las empresas y los clientes, pero se debe tener en cuenta las ocasiones en las que exista ausencia de suministro eléctrico y se debe contar con suministros alternos como segundas conexiones con baterías o grupos electrógenos.

- **Virus, troyanos y malware:** Este tipo de malware es un tipo de software no deseado que se debe eliminar.

- **Pérdida de datos:** Defectos en el código de origen o configuraciones defectuosas pueden llegar a causar modificaciones en la información que se almacena e incluso que se pierdan los datos, ante ello se puede tomar en cuenta las pruebas de las aplicaciones que se deseen usar antes de usarlas y realizar copias de seguridad en distintos puntos de procesamiento de información con el fin de poder recuperar lo perdido.

- **Ataques a las aplicaciones de los servidores:** Existe la posibilidad de que los hackers accedan a los datos aprovechando la vulnerabilidad del sistema operativo o de las aplicaciones que se ejecutan en el sistema operativo del equipo.

(Ríos, 2021) aborda a la seguridad activa y pasiva realizando una comparación con la seguridad vial que tiene como objetivo minimizar los

efectos de tránsito durante la circulación de automóviles y la seguridad activa se conforma principalmente por los elementos que intentar evitar que se produzcan accidentes como la educación vial, los frenos, neumáticos en buen estado, etc.; en cambio la seguridad pasiva se conforma por aquellos elementos que brindan seguridad durante el accidente así como los airbags, cinturones de seguridad, entre otros; en caso de la seguridad informática.

La seguridad activa es aquella que se conforma por aquellos elementos que intentan evitar ciberataques como los firewalls, sistemas antimalware, antivirus, sistemas de detección de intrusos, entre otros.

La seguridad pasiva es aquella que se conforma por aquellos elementos que minimizan los daños durante un ciberataque y ponen en marcha todos los mecanismos que involucran el bloqueo del ataque y la recuperación de la normalidad en el menor tiempo posible.

3.3.2.2. Cibercriminalidad

(Valdez, 2009) aborda al delito informático como aquellos hechos ilícitos que vulneran la seguridad y confidencialidad de un sistema informático, los archivos, documentos electrónicos, bases de datos, correos electrónicos y la red que son herramientas esenciales de las organizaciones y empresas cuya vulnerabilidad y violación de su confidencialidad se sanciona penalmente mediante la tipificación de delitos informáticos; en tanto la criminalidad informática se compone de delitos o conductas que atentan contra el soporte lógico de un sistema, contra el software o los datos y/o documentos relevantes almacenados en un procesador que pueden ser manipulados, hurtados, destruidos, etc. El cibercrimen en términos generales se puede entender como un comportamiento orientado a vulnerar, mediante operaciones electrónicas, la seguridad de sistemas computacionales o redes de computadoras; acciones como accesos no autorizados, daños a programas o datos, sabotajes computacionales, intercepciones no autorizadas de comunicaciones, espionajes computacionales pueden definir de mejor manera al cibercrimen y este puede categorizarse en:

- **Cibercrímenes violentos:** Ataques que pueden generar daños físicos a personas mediante el uso de redes de computadoras, acciones que incluyen al ciberterrorismo, amenazas de ataques, ciberespionaje, pornografía infantil, entre otros.

- **Cibercrímenes no violentos:** La principal característica de estos ataques son la no necesidad de contacto físico, se encuentra conformado por acciones como: Ciberrobo, ciberfraude, cibercrimen destructivo, entre otros.

Algunos de los delitos contra datos y sistemas informáticos que el estado peruano toma en cuenta y define son:

- **Acceso ilícito:** Aquel que accede sin permiso o autorización a la totalidad o a alguna parte del sistema informático que se realice a través de la vulneración de las medidas de seguridad que se establecen para bloquear dicho acceso.
- **Atentado contra la integridad de datos informáticos:** Aquel que intencionalmente daña, introduce, borra, deteriora, altera o suprime datos informáticos.

- **Atentado a la integridad de sistemas informáticos**: Aquel que intencionalmente inhabilita de manera total o parcial un sistema informático e impide la accesibilidad a este, obstaculiza o imposibilita su labor u operatividad.

- **Tráfico ilegal de datos:** Aquel que utiliza indebidamente una base de datos sobre una persona u organización para fines comerciales, trafico, venta, promoción o favorecimiento con información relativa a cualquier ámbito que corresponda a dicha persona u organización creando o no perjuicio.

- **Interceptación de datos informáticos:** Aquel que deliberadamente

intercepta datos informáticos de redes de transmisión informática y comunicaciones no públicas.

Si bien el término cibercrimen se usa de manera amplia, es correcto definir al cibercrimen como una actitud delictiva realizada en el ciberespacio que se agrava a conductas cuyo contenido ilícito se relaciona directamente a los intereses y bienes sociales existentes en el ciberespacio (Miró, 2012).

3.3.2.3. NIST Cybersecurity Framework (CSF)

(OEA, 2019) Ante el incremento del número de incidentes en ciberseguridad en los Estados Unidos, en el año 2012, el presidente Barack Obama emitió una orden en la que se encargó al NIST (Instituto Nacional de Estándares y Tecnologías) el desarrollo del Marco de ciberseguridad para la protección de infraestructuras críticas, algo que se conoce hoy en día como Cybersecurity Framework (CFS) y es una herramienta que permite la gestión de riesgos de ciberseguridad y se ajusta a cualquier tipo de organización sin importar el rubro al que se dedique si su organización y la principal innovación de esta herramienta fue que dejaba de lado estándares rígidos, además de ser simple y flexible; la estructura del CSF consta de tres componentes principales que son:

- **Framework core:** Que es un conjunto de actividades y resultados de ciberseguridad deseados que se organizan en categorías y se alinean con referencias informativas a estándares establecidos por la organización y se encuentra diseñado para actuar intuitivamente, además de actuar como una capa de traducción con el fin de utilizar un lenguaje simple y no técnico para apoyar a la comunicación entre equipos; el Core se conforma de tres partes que son: Funciones, Categorías y Subcategorías, además se incluyen 5 funciones de alto nivel que son: Identificar, proteger, detectar, responder y recuperar. Existen niveles más abajo como el que contiene 23 categorías que se dividen en las 5 funciones y se diseñaron con el objetivo de cubrir con más amplitud la ciberseguridad para una organización, además de ello hay 108 subcategorías que son declaraciones basadas en resultados

que brindan consideraciones para la mejora del programa de ciberseguridad.

- **Niveles de Implementación (Tiers):** Son el nivel en el que las experiencias acerca de la gestión de riesgos respecto a ciberseguridad de una organización exponen las características definidas en el marco.

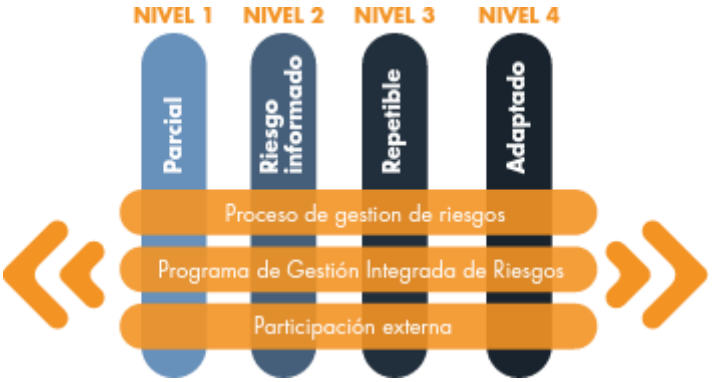

Figura 1 Niveles de implementación CSF

Fuente: (OEA, 2019)

Los niveles van desde el nivel parcial que es el nivel 1 al adaptativo que es el nivel 4 y muestran el grado de rigurosidad y a que grado se encuentran integradas las decisiones de riesgo de ciberseguridad, además en que grado la organización comparte y recibe información de fuentes externas.

- **Perfiles:** Los perfiles se definen como la línea única a la que una organización ajusta sus exigencias y objetivos institucionales, además de la pasividad al riesgo y sus recursos con respecto a los resultados que se desean obtener del Framework Core, estos perfiles se pueden usar con el fin de identificar oportunidades y mejorar la postura de ciberseguridad comparando un perfil actual con uno de objetivo.

Las funciones del CSF incluidas en el Framework Core son:

- **Identificar:** Desarrolla una comprensión organizacional con el fin de administrar los riesgos de ciberseguridad de los sistemas, personas, activos, datos organizacionales y capacidades; esta comprensión

ayuda a que los esfuerzos y los recursos que se suministran a las funciones críticas se encuentren orientados a la estrategia de administración de riesgos y necesidades comerciales de la organización.

- **Proteger:** Describe las medidas de ciberseguridad que son adecuadas para garantizar la entrega de servicios de las infraestructuras críticas.
- **Detectar:** Define las actividades que son necesarias para la identificación de eventos de ciberseguridad.
- **Responder:** Considera las acciones que serán necesarias ante un evento de ciberseguridad detectado, conteniendo el impacto de un potencial incidente.
- **Recuperar:** Considera las actividades necesarias para restaurar cualquier capacidad o asistencia que se hayan dañado debido a algún incidente de ciberseguridad.

Figura 2 Funciones del CSF
Fuente: (OEA, 2019)

3.3.2.4. Indicadores de compromiso (IOC)

Es posible combatir ataques sofisticados hoy en día gracias a las mejoras continuas que se hacen a los sistemas de gestión de eventos e información de seguridad (SIEMS), las mejoras se orientan a las técnicas de mitigación de ataque que a la vez han llegado a generar parámetros que

detectan patrones de amenaza o ataque en fase temprana, uno de ellos son los indicadores de compromiso (IOC) que ayudan a la detección de ataques al instante antes de que los daños sean causados (ManageEngine, 2021). El IOC se activa y muestra que existe un ataque a la infraestructura, en consecuencia a ello son una táctica favorable para la identificación de Malware compuestos de firmas de virus y la particularidad de esta estrategia es que es posible seleccionar piezas propias del virus para crear los indicadores de compromiso; una de las amenazas más conocidas es el Ransomware que es un código malicioso que tiende a secuestrar información en canje de bitcoin por el rescate, entre lo más frecuente se encuentra el Ransom- Criptolocker, Winlocker, Ransom-Locky-Criptowall, Teslacrypt, Torrent-locker; el Rasomware afecta de sobremanera a varios sectores de la industria como el educación, sectores gubernamentales, sectores financieros, sectores sanitarios y sectores públicos (Ponce, 2021).

Tabla 1 Tipos de indicadores de compromiso (IOC)

Tipo	Descripción
Artefactos Basados en Red	Son recibidos desde servidores, puertos, proxy server, entre los artefactos recolectados tenemos: captura de paquetes, estado de la red y sesiones.
Artefactos Basados en Host.	Son recibidos desde el equipo, entre los artefactos recolectados tenemos: el registro del sistema y el sistema de archivos.
Artefactos Basados en Red / IPs	Identificar las IPs del comando y control son claves para identificar una conexión maliciosa.
Artefactos Basados en Red / URL	Identificar las URLs asociadas a una Botnet y sus IPs relacionadas es punto clave en la detección, para su posterior bloqueo.
Artefactos Basados en Red/ Puertos y Servicio	Servicios como DNS, HTTP, TCP, UDP, ICMP, FTP, SSH son analizados con sus puertos relacionados, la mayoría puertos altos.
Artefactos Basados en Host/ Registro	Generar los IoCs de los cambios en el registro (Persistencia) es señal de una computadora infectada
Artefactos Basados en Host/ Procesos	La revisión de los procesos en estado running es un indicador clave para la identificación de Malware en el sistema incluye revisión de spawning process tree, carga de DLLs y parámetros utilizados.

Fuente: (Ponce, 2021)

3.3.2.5. Centros de operaciones de seguridad (SOC)

De acuerdo con (Morales, Moreno, & Ortigoza, 2014) un centro de operaciones (SOC) se define como una unidad concentrada al interior de una organización que se dedica de manera exclusiva a los temas estratégicos y operativos que se relacionan con los temas de seguridad informática, el equipo constituido en esta unidad realiza labores de monitoreo, aseguramiento y protección de los activos de la información mediante el uso de equipos tecnológicos.

El centro de operaciones se debe basar en las siguientes funciones:

- **Prevención:** Su función es minimizar la probabilidad de que se presenten incidentes, además de realizar constante vigilancia ante nuevos ataques que puedan afectar la seguridad mediante la implementación de medidas preventivas.

- **Detección:** Monitoreo constante con el propósito de detectar amenazas, vulnerabilidades y ataques que vulneran la seguridad.

- **Análisis:** Estudio de los incidentes que pudieron haberse presentado con el fin de diferenciar amenazas reales y falsos positivos.

- **Respuesta:** Los acciones que se realizan en contra de algún incidente que pretenda vulnerar la seguridad.

Para (Martínez, 2021) los SOC son importantes para la minimización de los costes ante eventos que puedan violar datos, debido a que no se limitan a ayudar a las organizaciones a responder ante dichos eventos con rapidez, sino que también mejoran de manera constante los procesos de detección y prevención. Existen diferentes tipos de SOC que son implementados de acuerdo a las necesidades de las organizaciones y las características de las empresas, que son:

- **SOC dedicado o autogestionado:** Modelo con personal e instalación dentro de las instalaciones de la organización.

- **SOC distribuido:** Mas acreditado como SOC cogestionado, este es un modelo que cuenta con componentes de un equipo dedicados a tiempo completo o parcial y que se contratan interiormente con el finde ejercer labores en conjunto con un proveedor de servicios de seguridad que se gestionan por terceros.

- **SOC gestionado:** Este modelo cuenta con un proveedor de servicios de seguridad gestionado por terceros que proporcionan todos los servicios.

- **SOC de mando:** Modelo que proporciona instrucciones acerca de amenazas y experiencias de seguridad en otras organizaciones o empresas, este SOC de mando no tiene participación en las operaciones de seguridad reales, sólo en la parte de inteligencia.

- **Centro de fusión:** Modelo que supervisa instalaciones que se centran en operaciones de seguridad, estos se consideran modelos de SOC avanzados y trabajan con equipos multidisciplinarios de las empresas para las operaciones de tecnologías de información y desarrollo de productos.

- **SOC multifunción:** Modelo que solo tiene una instalación que se dedica, además de personal interno, cumple funciones y encargos que se amplían a otras áreas importantes de la gestión de tecnologías de información.

- **SOCaas:** Modelo que se basa en un software que subcontrata algunas funciones del SOC a un proveedor en la nube.

La estrategia que se maneja en un centro de operaciones de seguridad tiene enfoque hacia la gestión de amenazas, además de la recolección de datos y análisis de los mismos para la detección de acciones que sean inseguras con el objetivo de implementar medidas de perfeccionamiento en la seguridad de una empresa u organización. Los compromisos primordiales de

un equipo SOC son:

- El hallazgo y la gestión de activos, son responsabilidades que implican conseguir información acerca de las herramientas, software, hardware y las tecnologías que se usan en la organización.

- La supervisión continua de la conducta que incluye los exámenes de todos los sistemas con el fin de efectuar medidas reactivas y proactivas ya que cualquier anomalía en la actividad se detecta de manera instantánea.

- Mantener registros de actividad con el fin de que los miembros del equipo SOC localicen e identifiquen acciones que pudieron haber dado lugar a las anomalías.

- La clasificación de la gravedad de las alertas ayuda a los equipos a avalar que las alertas más graves y urgentes sean tratadas primero.

- El desarrollo de medidas de seguridad con el fin de ayudar a los equipos SOC a estar al día y a estar preparados tanto para ataques nuevos y antiguos.

- La recuperación de incidentes a través de las copias de seguridad que permitan a las organizaciones recuperar los datos que se pudieron haber comprometido en algún evento de seguridad informática o ataque.

- El mantenimiento del cumplimiento que garantiza que los miembros del equipo SOC cumplan con las normas para la realización de los planes de negocio de la empresa.

- Las capacidades añadidas del SOC que bien podrían incluir a la ingeniería inversa, el análisis forense, la telemetría de red y el criptoanálisis de acuerdo a las necesidades de la organización.

La forma del funcionamiento del SOC después de la detección de una amenaza, se muestra en la siguiente figura de forma esquematizada.

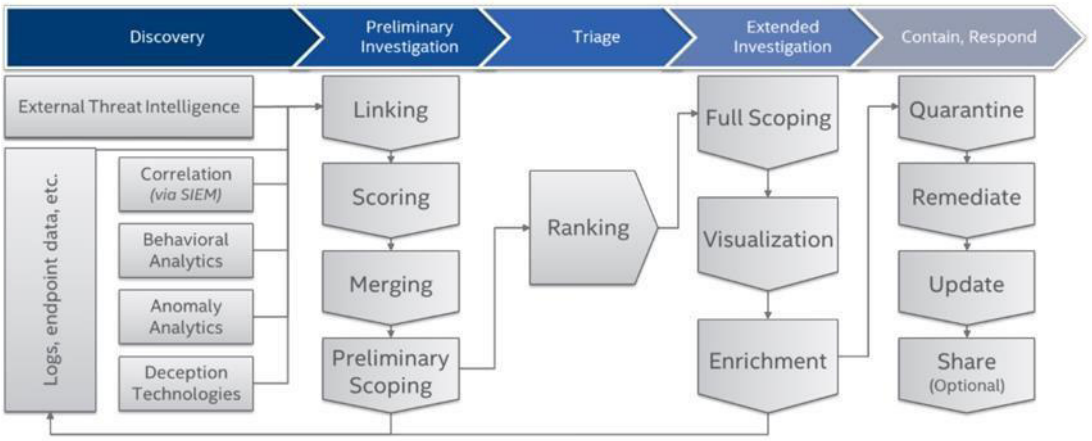

Figura 3 Funcionamiento de SOC

Fuente: (Martínez, 2021)

3.3.2.6. Inteligencia de amenazas

De acuerdo con (Ciberseguridad , 2022) la inteligencia de amenazas comprende el conocimiento basado en evidencia, contexto, mecanismos, indicadores y asesoramiento que se orienta a las acciones sobre una amenaza o peligro latente para los datos o activos informáticos; se utiliza con el fin de informar decisiones sobre la respuesta ante una amenaza o peligro.

De acuerdo con (Kapersky Lab , 2017) la inteligencia de amenazas comprende a un proceso de identificación y análisis de ciber amenazas y hace referencia a los datos que se coleccionan sobre una potencial amenaza con el fin de analizar dichos datos para comprender mejor las amenazas, básicamente la inteligencia de amenazas permite al usuario tomar decisiones sobre aspectos de seguridad de manera más rápida a través del uso de información, además fomenta las acciones proactivas en lugar de las reactivas en la lucha contra los ciber ataques; además la inteligencia de amenazas

desde un enfoque estratégico proporciona una visión sobre las tendencias de amenazas, tácticas y métodos que emplean los atacantes, así como sus motivos y atribuciones respondiendo de manera frecuente a una serie de preguntas que son:

- ¿Quiénes son los atacantes? ¿Cuál es su fin?
- ¿Qué grupos de amenazas se encuentran activos en la región?
- ¿Qué vectores de ataque emplean?
- ¿Cuál es la mejor forma de orquestar un ataque contra la organización?
- ¿De qué rutas e información se dispone cuando un atacante va contra la organización?
- ¿Se han llevado ataques anteriormente? ¿Cuál es grado de riesgo que se corre?
- ¿Qué acciones se deben llevar a cabo para reducir el perfil de riesgo?

Algunas de las plataformas existentes para el uso de inteligencia de amenazas son las que se muestran en la siguiente figura.

Nombre	Tipo	Año	Propietario	Sitio Web
Malware Information Sharing Platform (MISP)	Código abierto/ comunidad	2012	CIRCL	http://www.misp-project.org/ https://www.misp-project.org/communities/
Collaborative Research Into Threats (CRITs)	Código abierto	2014	MITRE	https://crits.github.io/ https://github.com/crits
Collective Intelligence Framework (CIF)	Código abierto	2012	CSIRT Gadgets Foundation	https://csirtgadgets.com/collective-intelligence-framework
Malware Attribute Enumeration and Characterization (MAEC v5)	Código abierto	2019	MITRE	http://maecproject.github.io/ https://github.com/MAECProject/
OpenCTI	Código abierto	2019	OpenCTI	https://github.com/OpenCTI-Platform/opencti
Open Threat Exchange (OTX)	Comunitario	2012	Alienvault	https://www.alienvault.com/open-threatexchange
X-Force Exchange	Comunitario	2015	IBM	https://exchange.xforce.ibmcloud.com/
Repositorio Común y Estructurado de Amenazas y Código Dañino (REYES)	Comercial	2017	CCN-CERT	https://www.ccn-cert.cni.es/soluciones-seguridad/reyes.html

Figura 4 Plataformas de inteligencia de amenazas

Fuente: (Barrera, Dorvigny, & Montesino, 2021)

Comprender la información con la que se cuenta permite el desarrollo de un análisis de riesgos exhaustivo y la comunicación de escenarios claros del riesgo para la organización, además con ello se tiene un buen fundamento

para la justificación de la inversión en programas, tecnología y personal; algunos informes de inteligencia que se ofrecen por empresas especializadas en inteligencias de amenazas son las que se muestran en la siguiente figura.

Tipo de informe	Inteligencia proporcionada	Caso de uso
APT Intelligence Reporting	• Descripciones de tácticas y métodos usados por los atacantes en campañas de ciberespionaje con objetivos intersectoriales • Los perfiles de los actores de amenazas con las TTP (Tácticas, Técnicas y Procedimientos) que usan • Cotejar los TTP asociados con MITRE ATT&CK, una base de conocimiento de TTP adversarios basada en experiencias del mundo real	• Comprender los actores de amenazas que acechan a su industria o región y los TTP que usan • Identificar qué información y sistemas están en riesgo, el impacto potencial al verse comprometidos y cómo dar prioridad • Ajustar las estrategias de la seguridad de la información, planear y justificar las inversiones en tecnología, personal y programas que cubran posibles vectores de ataque
Financial Threat Intelligence Reporting	• Descripciones de tácticas y métodos usados por los que atacan el sector financiero • Información sobre ataques en infraestructuras específicas, como cajeros o terminales TPV • Información sobre herramientas adaptadas para atacar redes financieras que usan, desarrollan y venden los cibercriminales en comunidades y foros de la Darknet de diferentes lugares	• Identificar a los adversarios que vayan tras instituciones financieras y los TTP que usan • Identificar la información y sistemas en riesgo, el impacto potencial de verse comprometido y cómo dar prioridad • Ajustar las estrategias de seguridad de la información, planear y justificar inversiones en tecnología, personal y programas que cubran posibles vectores de ataque
Customer-specific Threat Intelligence Reporting	• Identificación pasiva del perímetro de red, servicios disponibles y vulnerabilidades existentes • Análisis personalizado y análisis de exploits • Identificación, monitoreo y análisis de cualquier muestra de malware activa o no que vaya tras su organización • Filtrado de información y datos • Amenazas phishing que van tras las marcas de los clientes • Evidencia de amenazas y actividad botnet que amenacen a los clientes, socios y proveedores de la empresa • Análisis específico de la industria que incluye los TTP relevantes	• Garantizar la disponibilidad y correcta asignación de recursos para mitigar los errores de seguridad identificados • Informar de auditorías de compra de terceros para contrarrestar los ataques en la cadena de suministro • Ajustar las políticas y controles para mitigar posibles amenazas internas • Aumentar el conocimiento en seguridad del personal interno desarrollando un programa específico basado en hechos (p. ej. Credenciales corporativas comprometidas por servicios de terceros) • Mitigar los posibles daños de reputación monitoreando el uso no autorizado de las marcas de la empresa con fines phishing • Planificar y justificar las inversiones tecnológicas, de personal y en programas que cubran los vectores de ataque relevantes

Figura 5 Informes de inteligencia de amenazas

Fuente: (Kapersky Lab , 2017)

En la figura anterior, se puede observar que ATP Inteligence Reporting proporciona una inteligencia ante descripciones de tácticas y métodos usados ante atacantes que tienen fines de ciberespionaje, estableciendo casos de uso como la identificación de información y sistemas en riesgo, impactos potenciales y estrategias de seguridad de información; en tanto, Financial Threat Intelligence Reporting proporciona una inteligencia de descripciones de tácticas y métodos que usan los atacantes del sector financiero, información sobre ataques en cajeros e información en herramientas que usan los atacantes contra redes financieras, estableciendo casos de uso como la

identificación de oponentes que atacan entidades financieras, identificación de sistemas de riesgo, impactos potenciales y ajuste de estrategias de seguridad; Customer Specific Threath Intelligence Reporting proporciona una inteligencia ante la identificación pasiva de los perímetros de red, servicios disponibles y vulnerabilidades existentes, análisis personalizado de exploits, identificación, monitoreo y análisis de cualquier muestra de malware activas, filtrados de información y datos y amenazas de pishing que van tras diversas marcas estableciendo casos de uso como garantizar la disponibilidad y correcta asignación de recursos, con el fin de mitigar los errores de seguridad, informes de auditorías de compra de terceros, ajustes de políticas y controles para la mitigación de amenazas internas e incrementos de conocimientos en seguridad del personal.

3.3.2.7. Gestión de vulnerabilidades

De acuerdo con (Tenable, 2022) la gestión de vulnerabilidades es un proceso de tipo continuo que contempla la detección, monitoreo, mitigación, corrección de activos y tácticas de defensa que se necesitan para proteger a la organización de ciber ataques.

De acuerdo a (AGESIC, 2022) se define a la vulnerabilidad de seguridad como un fallo técnico o deficiencia del sistema que es capaz de permitir el acceso ilegitimo de a la información o al acceso de operaciones no autorizadas de manera remota; el proceso de gestión de dichas vulnerabilidades se encuentra comprendido por siete pasos que son:

- **Identificación de activos:** Una forma de tener identificados todos los activos existentes en una organización es la elaboración de un inventario de todos ellos con el fin de mantenerlos protegidos a través de controles adecuados; no es necesario un inventario exhaustivo de cada activo, solo tenerlos identificados en grupos que puedan requerir los mismos controles, como por ejemplo agrupar sistemas de configuraciones similares. Como identificadores de clasificación se pueden agrupar los activos cuando:

- Son del mismo tipo
- Tienen configuraciones similares
- Se encuentran integradas en la misma red
- Se encuentran sujetas a las mismas condiciones de infraestructura
- Usan las mismas aplicaciones
- Tienen los mismos requisitos de protección

Si se agrupan los activos se debe tener cuidado en cómo se hace ya que si se hace de manera incorrecta se da lugar a vulnerabilidades de seguridad.

- **Planificación de análisis de vulnerabilidades:** Las organizaciones deben realizar evaluaciones constantes acerca de las vulnerabilidades ya que la organización debe ser consciente de los riesgos que acarrean dichas vulnerabilidades.

- **Ejecución de análisis de vulnerabilidades:** Se debe hacer uso de un sistema de evaluación de vulnerabilidades automatizado (VAS) con el fin de identificar las vulnerabilidades de sistemas, equipos de TI de la organización. Cuando se haga uso del VAS es necesario:

  - Evaluar los sistemas desde una perspectiva externa y también desde una perspectiva interna.
  - Supervisar las cuentas que se estén utilizando para la ejecución del análisis de vulnerabilidades para buscar actividades inusuales.
  - Realizar escaneos de las redes y de los sistemas conocidos para descubrir dispositivos potencialmente desconocidos.
  - Tener en cuenta que el VAS puede generar resultados inesperados que pueden incluir la corrupción de datos.
  - Ejecutar el VAS con las credenciales auténticas para la realización de la evaluación del host, no un escaneo no autenticado.

- **Clasificación de vulnerabilidades encontradas:** El software de

evaluación de vulnerabilidades que se use brindará una clasificación de gravedad de los problemas, pero este no debe ser considerado como un resultado definitivo ya que no tomará en cuenta ningún riesgo o circunstancias atenuantes. El Common Vulnerability Scoring System (CVSS) es un marco abierto que permite la comunicación de las características y gravedad de las vulnerabilidades del sistema ya que al asignarle puntuaciones numéricas ayuda al proceso de clasificación de las mismas, pero no debe asignársele una puntuación arbitraria por encima de las vulnerabilidades que deben corregirse y no tomar en cuenta puntuaciones sin tener en cuenta las prioridades o mitigaciones específicas de la organización; usualmente las categorías en las que se clasifican las vulnerabilidades son:

- **Corregir:** Aquellas en las que se debe aplicar un parche o una configuración de mitigación.
- **Reconocer:** Aquellas que no deben ser corregidas de inmediato y se les debe asignar una fecha de revisión.
- **Investigar:** Son aquellas de las que se desconoce el costo de resolver o que tiene varios modos solucionar de modo que pueda requerir un tiempo determinado para observar cuál de las soluciones funciona mejor.

- **Priorización de vulnerabilidades:** La priorización de vulnerabilidades se debe realizar centrándose en que:
  - Son accesibles para una determinada cantidad de atacantes
  - El impacto que pueden tener si se introducen en la unidad operativa de la organización.

- **Remediación:** En esta etapa se busca implementar los parches que corresponden a cada vulnerabilidad identificada y clasificada en estado “corregir” del orden de prioridad.

- **Validación:** Se debe validar el resultado para ver si se redujeron las vulnerabilidades asignando puntajes promedios de vulnerabilidad,

cantidad de vulnerabilidades, etc.

Figura 6 Proceso de gestión de vulnerabilidades
Fuente: (AGESIC, 2022)

3.3.2.8. Monitoreo de plataformas

De acuerdo con (NEOSECURE, 2022) el monitoreo de seguridad que se asocia con los controles para la detección es una disciplina que ha brindado compañía a la ciberseguridad ya desde hace mucho tiempo y a través de los años ha ido evolucionando añadiendo nuevas técnicas y sistemas de apoyo que hacen de esta actividad menos compleja; su importancia se observa en que la totalidad de los modelos y marcos de seguridad como el ISO 27001, NIST o PCI requieren del monitoreo que consiste en un equipo que tiene la función de alertas que provienen de una previa clasificación generalmente un SIEM, este es un proceso sistemático que observa la validación de alerta para determinar si es real o es un falso positivo. El monitoreo puede ser:

- **Perimetral:** Este es uno de los más tradicionales y requiere la observación de eventos de sistemas como firewalls, IPSs, WAFs, URL,

entre otros; usualmente la cantidad de eventos es elevada al igual que la tasa de falsos positivos.

- **De abuso de usuarios:** Esta tiene origen en la red interna que usualmente considera al escape de información o tentativas de acceso no autorizado a sistemas.

- **De fraude:** Este es parcialmente complejo y tiene semejanzas al de abuso de usuarios, se genera en función a un proceso de negocio y a sistemas que son muy propios del mismo, como en sistemas ERP, de cuenta corriente, plataformas de clientes, etc.

- **Aplicado en ambientes específicos:** Nuevos ambientes como redes OT o la nube que requieran exigencias especiales, como por ejemplo los que requieran usar sistemas determinados para dichos ambientes que comprendan sistemas, protocolos que se integren adecuadamente a estos.

- **Aplicado ante amenazas variadas:** Se aplica ante amenazas persistentes (APT) que por su naturaleza son muy sofisticadas y requieren de técnicas variadas.

3.3.2.9. Proceso de análisis forense digital

De acuerdo con (López, 2007) el proceso de análisis que permite identificar, recuperar, reconstruir y analizar evidencias de lo ocurrido en los sistemas informáticos se refiere al análisis forense digital que es la disciplina que se aplica tanto para la investigación de delitos relacionados con las tecnologías de información y comunicaciones, el autor define de manera formal al análisis forense digital como: *"Un conjunto de principios y técnicas que comprende el proceso de adquisición , conservación, documentación, análisis y presentación de evidencias digitales que de haber llegado el caso puedan ser aceptados legalmente en un proceso judicial"* . Dentro del proceso de análisis forense digital (AFD) se destacan fases que son:

- **Identificación de incidente:** Ante un ataque no se debe perder la calma y se debe asegurarse que no se trata de un problema de hardware o software de la red o servidor, posterior a ello se debe descubrir las señales de ataque realizando actividades que no comprometan la evidencia, para ello existen una gran cantidad de utilidades que pueden ser:

  - Interpretación de comandos en modo consola
  - Enumeración de puertos TCP y UDP abiertos y aplicaciones asociadas
  - Listado de usuarios conectados a la red local y remota del sistema
  - Obtención de fecha y hora del sistema
  - Enumeración de procesos activos, recursos que se utilizan y usuarios y aplicaciones que se lanzaron
  - Enumeración de direcciones IP del sistema y mapeo de las direcciones físicas
  - Búsqueda de ficheros ocultos o eliminados
  - Visualización de registros y logs del sistema
  - Visualización de configuración de seguridad del sistema
  - Generación de funciones hash de ficheros
  - Leer, copiar y escribir a través de la red
  - Realizar copias bit-a-bit de discos duros y particiones
  - Análisis de trafico de red

- **Recopilación de evidencias:** Una vez que se tiene la certeza de que los sistemas informáticos han sido atacados se debe decidir cuál será la prioridad:

  - Tener nuevamente operativos los sistemas
  - Realizar una investigación forense detallada

  La recopilación de evidencias que realice el equipo de expertos comprenderá: El método de entrada al sistema, la actividad de los

intrusos, su identidad y origen, además de la duración del compromiso y la toma de precauciones para evitar la alteración de evidencias durante el proceso de recolección; usualmente mientras se mantenga el equipo “vivo” se comienza a recopilar evidencias siguiendo un orden de mayor a menor volatilidad, orden que se sigue de acuerdo a:

- Registros contenidos en caché
- Contenidos de memoria
- Estado de conexiones de red
- Estado de procesos de ejecución
- Contenido de sistema de archivos
- Contenido de otros dispositivos

- **Preservación de evidencia:** Una vez que se tiene la evidencia se ejecuta un proceso conocido como la cadena de custodia en el que se establecen los encargos y controles a cada una de las personas que puedan manipular la evidencia, además se debe tener preparado la documentación que contenga información de los datos personales de los comprometidos en el proceso de manipulación de copias, desde su impresión hasta su almacenamiento

- **Análisis de la evidencia:** Una vez que se tengan las evidencias recopiladas y almacenadas de forma correcta se procede con el análisis forense propiamente dicho cuyo fin es reconstruir todos los datos disponibles de la línea temporal en la que sucedió el ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque hasta su descubrimiento.

- **Documentación y presentación de resultados:** Inmediatamente el incidente se haya descubierto, es transcendental iniciar con la toma de datos de las actividades que se lleven a cabo, cada paso tiene que ser registrado con la fecha desde que se descubre el incidente hasta que finalice el proceso de análisis forense.

3.3.3 Definición de términos

- **QRadar:** Plataforma SIEM de IBM adquirido por la entidad financiera.
- **Graylog (SERVICIO CLOUD -ANALIZADOR):** Plataforma opensource elegida para trabajar como SIEM y hará funciones similares que Qradar.
- **Logstash (SERVER COLLECTOR):** Plataforma opensource para recibir y clasificar logs, en el servicio se puso el nombre de "Server Collector".
- **PRTG:** Plataforma para las alertas de los servidores a nivel de disco, memoria, CPU, conectividad.
- **GRAFANA (SERVICIO CLOUD-PORTAL):** Plataforma que sirve para generar dashboard de monitoreo y gestión, en el servicio permitía mostrar indicares gráficos ejecutivos al cliente como a su vez nos permitía gestionar alertas de toda la infraestructura SERVICIO CLOUD.
- **Conexión SITE to SITE:** Alternativa optada para comunicar la infraestructura cliente con el servicio.
- **TICKETERA (SERVICIO CLOUD-MONITOR):** Nombre de la herramienta de gestión de tickets.
- **TICKETVULN:** Módulo de gestión de vulnerabilidades de TICKETERA.

3.4 Procedimiento

3.4.1 Tipo de investigación

La investigación realizada y plasmada en el presente informe es de tipo aplicada y de alcance descriptivo, debido a que muestra la aplicación de conocimientos acerca de la Implementación de servicio de centros de

operaciones de ciberseguridad (CyberSoc) con Plataformas Opensource a entidades financieras en la solución de problemas de ciberseguridad y de alcance descriptivo debido a que solo se limita a describir el proceso y los resultados obtenidos con la implementación.

3.4.2 Diseño de la investigación

El diseño de la investigación se compone del análisis de las características técnicas, tomando en cuenta la situación actual del cliente y la infraestructura necesaria para la implementación del servicio de centro de operaciones de ciberseguridad (CyberSoc) con plataformas OpenSource en la entidad financiera.

3.4.2.1 Situación actual del cliente

La entidad financiera tenía la necesidad de gestionar y complementar su infraestructura TI en términos de ciberseguridad ante la presencia de ataques de seguridad. Como proveedor la empresa Royal ITC planteó ofrecer un servicio cyberSOC el cual consta de los siguientes subservicios:

1. Monitoreo de plataformas: este subservicio utilizó las siguientes herramientas:
    - PRTG
    - TICKETERA (SERVICIO CLOUD-MONITOR)
    - GRAFANA (SERVICIO CLOUD-PORTAL)

2. Gestión de vulnerabilidades: este subservicio utilizó las siguientes herramientas:
    - Kali server
    - GRAFANA (SERVICIO CLOUD-PORTAL)

3. Respuesta ante incidentes: Este subservicio es procedimental.

4. Gestión y correlación de eventos: Este subservicio utilizó las siguientes herramientas:
    - QRADAR
    - LOGSTASH (SERVER COLLECTOR)
    - GRAYLOG (SERVICIO CLOUD-ANALIZADOR)
    - GRAFANA (SERVICIO CLOUD-PORTAL)

5. Gestión de análisis forense: Este subservicio es procedimental

En la siguiente figura se muestra para mayor entendimiento los subservicios mencionados líneas arriba, donde la parte de detección se realizaría el monitoreo de plataformas, en la parte de análisis se aplicaría la gestión de vulnerabilidades, gestión y correlación de eventos y gestión de análisis forense, mientras que en la parte de respuesta se realizaría la respuesta ante incidentes.

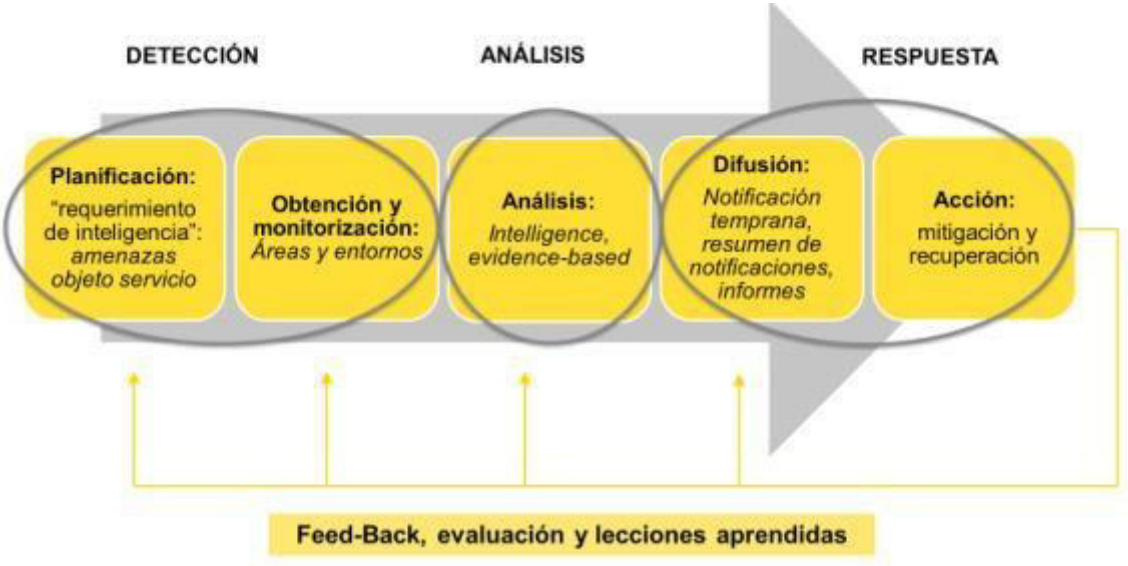

Figura 7 Proceso cyberSOC

Fuente: (Blanco, 2017)

3.4.2.2 Componentes de Arquitectura

Se hizo uso de los siguientes componentes de software y hadware para el logro del objetivo principal:

Conexión SITE to SITE: La VPN SITE to SITE permite a Royal ITC establecer una conexión segura a la LAN del cliente a través de internet, a su vez el cliente puede acceder al dashboard y al sistema de gestión de tickets mediante la Red Privada Virtual (VPN); los parámetros de VPN se muestran en la siguiente tabla.

Tabla 2 Parámetros VPN

Parámetros del VPN Device	Información de Cliente	Royal ITC
VPN Device IP Address (Peer)	183.66.188.22	200.27.74.34
VPN Device Version	Checkpoint R88.22	Huawei Cloud
Encryption domain Peer	173.23.110.10/38	175.15.1.0/21
	174.22.110.60/38	
	174.21.110.60/38	

Fuente: Elaboración propia

Los parámetros de conexión para el establecimiento de la VPN se muestran en la siguiente tabla.

Tabla 3 Parámetros de conexión

VPN – Fase 1 (IKE)	Información de Cliente	Royal ITC
Encryption Algorithm	AES-256	AES-256
Hashing Algorithm	SHA256	SHA2-256
Authentication Method	Pre-Shared Key	Pre-Shared Key
Diffie-Hellman group	Group-2 (1024 bits)	Group 2
Renegotiate IKE SA every	86400 seconds (1440 minutes)	86400 seconds
Encryption Method	IKEv1	IKEv1
VPN – Fase 2 (IPSec)	**Información de Cliente**	**Royal ITC**
Encryption Algorithm	AES-256	AES-256
Hashing Algorithm	SHA256	SHA2-256
Aggressive Mode Support	NO	NO
Key Exchange For Subnet	NO	

Use perfect Forward Secrecy	NO	
Support Site to Site Compression	NO	
Renegotiate IPSEC SA every	3600 seconds	3600 seconds
Transfer Protocol	ESP	ESP

Fuente: Elaboración propia

Las políticas de firewall para el establecimiento de la VPN, se muestran en la siguiente tabla.

Tabla 4 Políticas de Firewall

Política	IP Host Origen	H. Origen	IP Host Destino	H. Destino	Protocolo	Puerto	URL
Ejemplo	**10.10.10.10**	**host1.cliente.pe**	**200.100.100.200**	**host2.E.com**	**TCP**	**80**	
1	171.17.1.0/21		171.23.110.10/35		TCP	80 443 22	Server Collector
2	171.17.1.0/21		171.23.110.20/35		TCP	80	PRTG
3	171.23.110.10/35		171.17.1.0/21		TCP	10051 12201	Server Collector
4	171.23.110.10/35		171.17.1.0/21		UDP	60000 - 60020	Server Collector
5	171.17.1.0/21		171.23.110.10/35		ICMP	-	Server Collector
6	171.17.1.0/21		171.23.110.40/35		TCP	22 80 443 3350	Escáner de vulnerabilidades
7	171.23.112.0/21		171.17.1.0/21		TCP	80 443	Ticket | Dashboard | TICKETVULN
8	171.23.112.0/21		171.17.1.0/21		TCP	20 21	File Server (Reporte de Monitoreo)

Fuente: Elaboración propia

El Server Collector envía todo el tráfico del Logstash hacia la infraestructura SERVICIO CLOUD a través de la Red Privada Virtual (VPN), se muestra el diagrama de conexión del establecimiento de la VPN en la siguiente Figura.

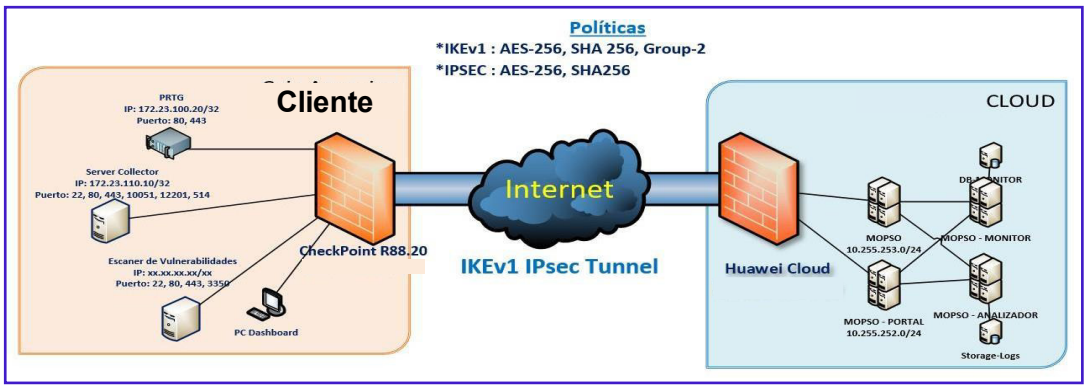

Figura 8 Diagrama de conexión de conexión VPN

Fuente: (Royal ITC,2021)

Herramienta de gestión de Tickets: Los servicios que se soportan con el aplicativo **"e tickets"** de desarrollo propio, fueron: La gestión de incidentes de TI y la gestión de incidentes de seguridad de la información, el proveedor Royal ITC entregó al cliente las credenciales para que este pueda acceder también al sistema de gestión de tickets a través de la conexión VPN, el diagrama de conexión a la herramienta se muestra en la siguiente Figura.

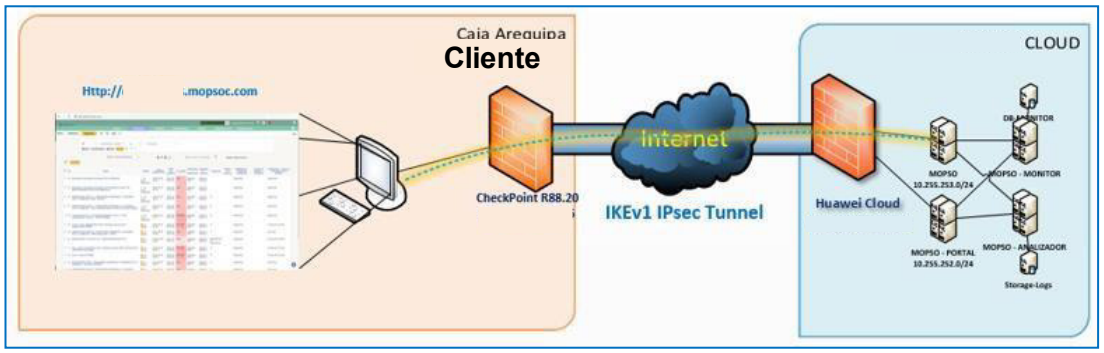

Figura 9 Diagrama de conexión a la herramienta "Gestión de Tickets"

Fuente: (Royal ITC,2021)

TICKETVULN: Esta herramienta se conoce como el sistema de gestión de vulnerabilidades (TICKETVULN), que permite el registro y seguimiento de las vulnerabilidades que se identifican a través del escaneo de vulnerabilidades, el diagrama de conexión a la herramienta de gestión de vulnerabilidades se muestra en la siguiente Figura.

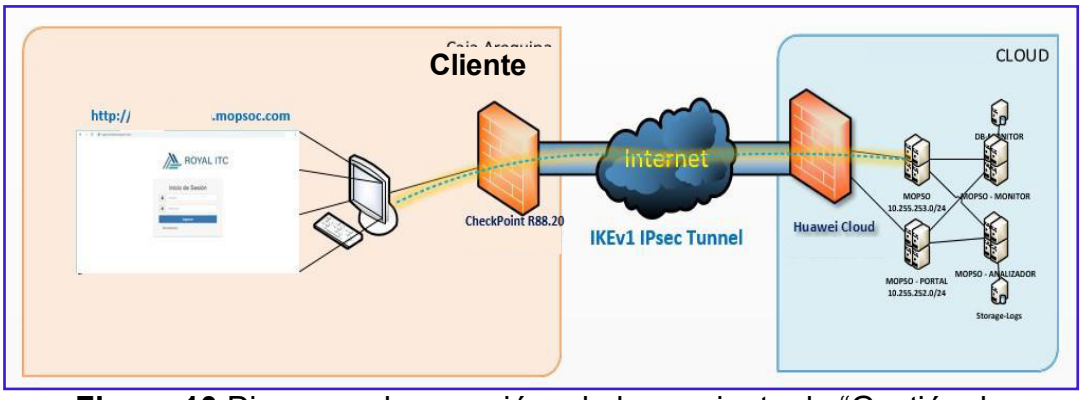

Figura 10 Diagrama de conexión a la herramienta de “Gestión de vulnerabilidades”

Fuente: (Royal ITC,2021)

Dashboard- Grafana: Dashboard es un aplicativo web que se basa en la herramienta Grafana que permite monitorear los equipos del cliente que se especifican en el contrato; además es importante resaltar que Grafana es una herramienta que permite mezclar diferentes fuentes de datos en un silo gráfico, especificando el origen de datos e integrando fuentes de datos personalizados; es así que el cliente también tenía acceso al Dashboard con las credenciales que le hizo entrega el proveedor y a través de la conexión VPN; se muestra en la siguiente Figura el diagrama de conexión al Dashboard.

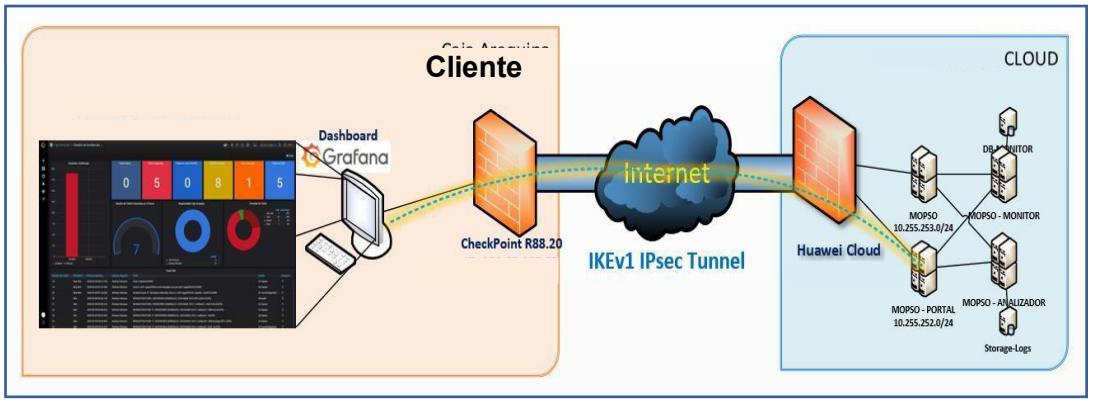

Figura 11 Diagrama de conexión Dashboard

Fuente: (Royal ITC,2021)

Escáner de Vulnerabilidades: Se contó con tres herramientas para el escaneo de vulnerabilidades, una de ellas facilitada por el cliente que fue la herramienta **"Nessus vulnerability scannery"** y por parte de Royal ITC **"Kali Linux"** y **"OpenVAS"**. Kali Linux es una distribución de Linux basada en Debian que se orienta a pruebas avanzadas de penetración y auditorias de seguridad, esta contiene herramientas que ayudan en el cumplimiento de diversas tareas de seguridad de información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa, también cuenta con escáneres de vulnerabilidades como:

- Nikto
- Owasp ZAP
- Dirbuster Dirb
- Burp Suite
- SQLmap
- Nmap
- Whois
- WPScan
- Scripts de desarrollo propio

Kali Linux fue instalado en el servidor que proveyó el cliente y se ubicó dentro de la infraestructura de la red del cliente, el servidor de escáner de

vulnerabilidades tenía acceso a todas las redes y equipos a escanear. OpenVAS es un escáner de vulnerabilidades que tiene capacidades que incluyen pruebas de carácter no autenticado, protocolos industriales variados y de internet de alto y bajo nivel, ajustes de rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad, esta herramienta fue instalada en el servidor Kali Linux en la infraestructura del cliente, las formas de realizar los escaneos eran dos: La primera desde la infraestructura de SERVICIO CLOUD y la segunda desde las instalaciones del cliente, el diagrama de conexión de vulnerabilidades se muestra en la siguiente Figura.

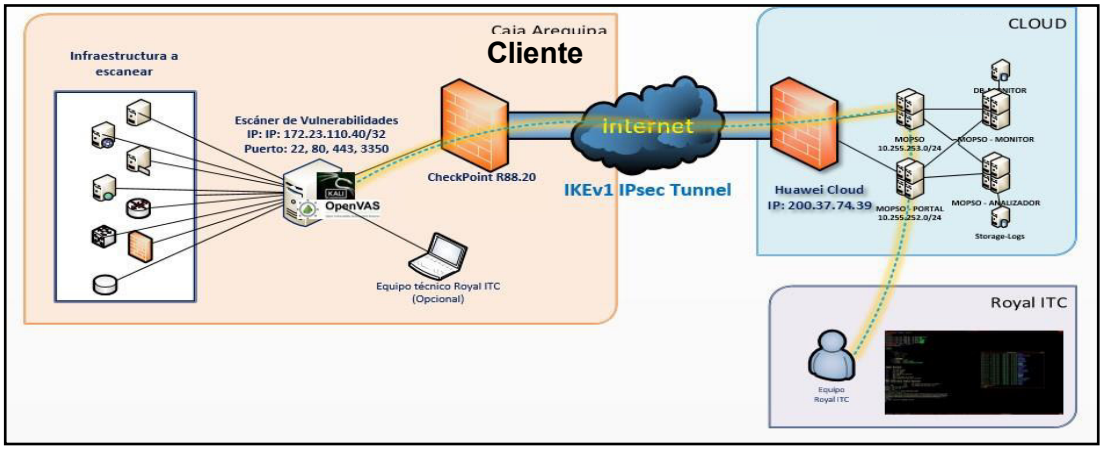

Figura 12 Diagrama de conexión del escáner de vulnerabilidades

Fuente: (Royal ITC,2021)

3.4.2.3 Integración de Componentes de Arquitectura

El proveedor Royal ITC validó con el apoyo del cliente la información de los logs generados y recibidos desde los equipos de la infraestructura del cliente hacia el QRadar que permite que sean recibidos y procesados correctamente por Logstash.

Integración QRadar- Logstash: Cuando la información es recibida de los Logs por QRadar a Logstash, se inició la configuración del proceso de envío al SERVICIO CLOUD para el consumo y muestra en el dashboard. El

diagrama de integración de la herramienta SIEM QRadar y Logstash se muestra en la siguiente Figura.

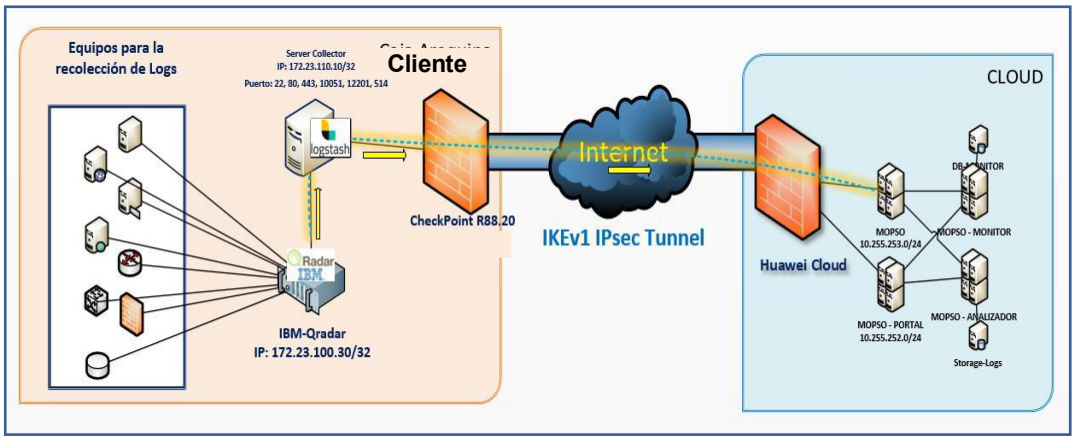

Figura 13 Diagrama de integración QRadar- Logstash

Fuente: (Royal ITC,2021)

Integración de la herramienta PRTG-Grafana: En el dashboard se podían visualizar los equipos que eran monitoreados por la herramienta PRTG y además de ello el cliente propuso la visualización de equipos que tenían alto grado de criticidad o eran especiales; para consumir la información de la herramienta PRTG, el proveedor Royal ITC requirió los accesos necesarios para la integración de la API de PRTG a Grafana y dependiendo de lo que el cliente necesitara ver, Royal ITC solicitaría a un usuario permisos de lectura o un usuario administrador y para casos especiales se solicitó un usuario de la base de datos de la herramienta PRTG para la realización de consultas específicas.

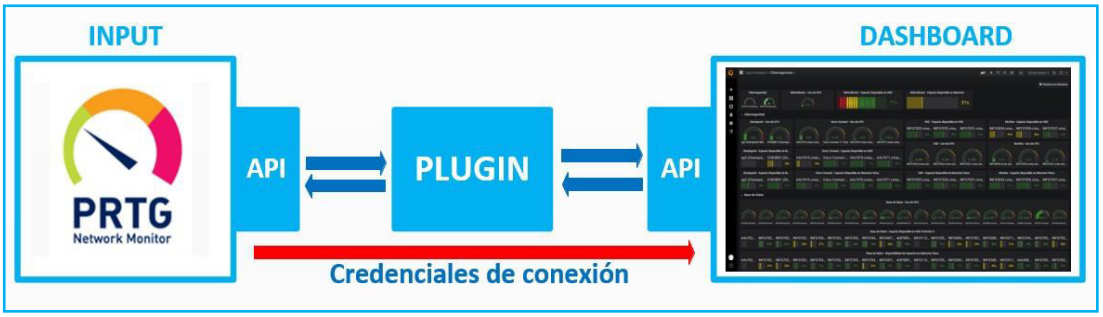

Figura 14 Diagrama de integración API de PRTG- Grafana

Fuente: (Royal ITC,2021)

Dashboard de correlacionador de eventos Graylog- Grafana: De acuerdo a la lista de casos de uso proporcionados por el cliente y los casos proporcionados por el proveedor Royal ITC, se implementaron progresivamente en la herramienta de gestión de correlación de eventos y alertas de seguridad que se visualizaban en el dashboard.

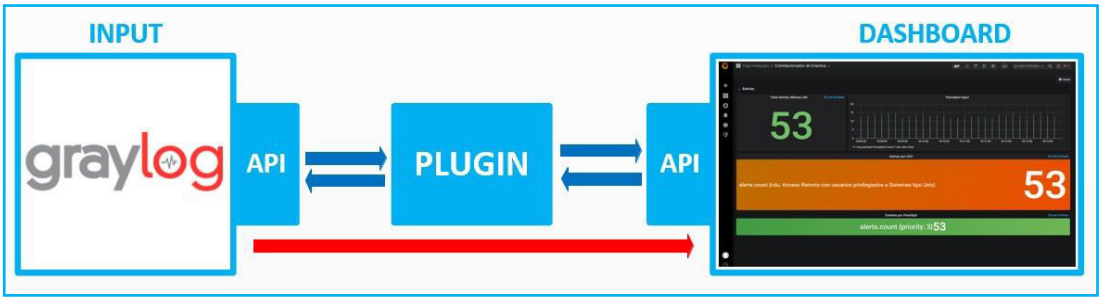

Figura 15 Diagrama Correlacionador de Eventos- Grafana

Fuente: (Royal ITC,2021)

Integración de la herramienta TICKETERA- Grafana: El dashboard hace posible realizar el seguimiento de los tickets asignados a los responsables de cada activo, fechas de asignación, prioridad, categoría, usuario asignado, etc.

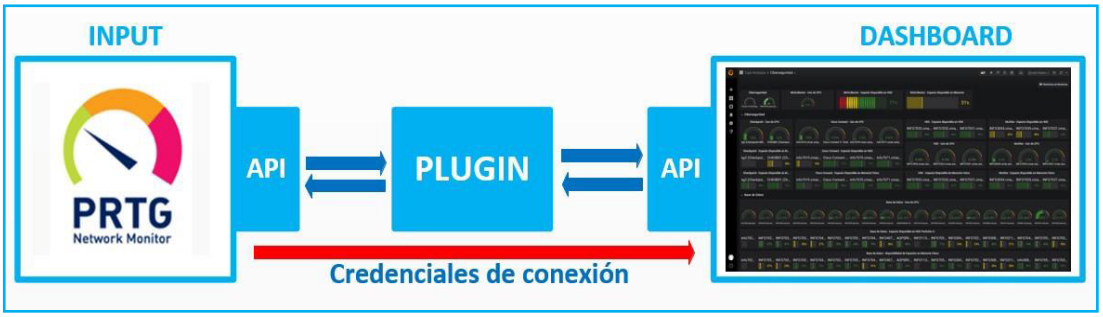

Figura 16 Diagrama Gestión de Tickets- Grafana

Fuente: (Royal ITC,2021)

Integración de la herramienta de TICKETVULN – Grafana: El dashboard hace posible el seguimiento de las vulnerabilidades que se registran al aplicativo "TICKETVULN"; el dashboard permite visualizar el tipo de vulnerabilidad, el estado de la vulnerabilidad, tiempo de cierre, área, impacto, etc.

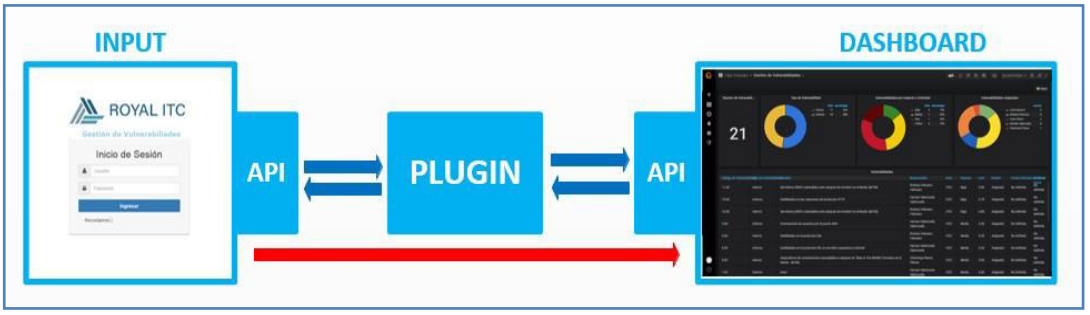

Figura 17 Diagrama Gestión de Vulnerabilidades- Grafana

Fuente: (Royal ITC,2021)

Integración Forense y Grafana: El cliente debía definir lo que desea visualizar en el dashboard y el proveedor previo acuerdo con el cliente proponía un prototipo visual o modelo de cómo se mostraría dicha información en el dashboard y recibiría la confirmación de los indicadores a mostrar en el dashboard.

Integración inteligencia de amenazas y Grafana: El cliente debía

definir lo que desea visualizar en el dashboard y el proveedor previo acuerdo con el cliente proponía un prototipo visual o modelo de cómo se mostraría dicha información en el dashboard y recibiría la confirmación de los indicadores a mostrar en el dashboard.

3.4.3 Requerimiento de equipamiento y software para implementación

Los tipos y características mínimas de los equipamientos necesarios del cliente fueron:

Server Collector

- CPU: 4 Cores
- RAM: 8 GB
- Almacenamiento: 500 GB

Escáner de Vulnerabilidades

- CPU: 4 Cores mínimo, recomendado 8 Cores
- RAM: 16 GB mínimo, recomendado 32 GB
- Almacenamiento: 500 GB

Las características del software requerido en los equipos del cliente fueron:

Server Collector

- OS: Debian o Red Hat
- Servicio SSH activo
- Username y password para ingresar (root)

Agente de monitoreo del server Collector

- Instalación de Zabbix y el proveedor debió proporcionar configuración respectiva una vez instalada
- Instalación y configuración de syslog para él envió del log al Server Collector

Escáner de vulnerabilidades

- Kali Linux 2020
- Acceso
- Servicio SSH activo

3.4.4 Procedimiento de implementación

El procedimiento de implementación de la de servicio de centro de operaciones de ciberseguridad (CyberSoC) con plataformas opensource en la entidad financiera, se muestra en el Anexo 08 del presente informe.

Respecto al monitoreo de plataformas, este se realizó usando la herramienta PRTG, la empresa realizó el monitoreo considerando la configuración establecida el cliente sin realizarle ningún cambio. El monitoreo se realizó mediante la conexión VPN desde la infraestructura SERVICIO CLOUD hacia el PRTG, para el cual el cliente entregó un usuario y password para otorgar acceso a Royal ITC y para dar inicio al monitoreo del PRTG, el cliente proporcionó a Royal ITC la configuración de la arquitectura del servidor PRTG y el estado actual de la configuración del PRTG como parte del levantamiento de información hacia Royal ITC.

Respecto a la gestión de vulnerabilidades se formularon planes de acción tanto para el proveedor y para el cliente para el correcto desarrollo del procedimiento, se muestran dichos planes en las tablas mostradas en el ANEXO 01 y en las figuras 19 y 20 del ANEXO 08.

Respecto al procedimiento de respuesta ante incidentes, se establecieron metodologías para que el cliente pueda tener el conocimiento para reportar y generar oportunamente los incidentes que se relacionaran con los activos de seguridad de la información y activos de TI que se muestran en el ANEXO 02 y en las figuras 21 Y 22 del ANEXO 08.

Respecto al procedimiento de gestión y correlación eventos, se configuró y se hizo uso de graylog posterior al establecimiento de casos de uso como:

- Detección de conexiones entrantes al cliente desde fuera del Perú.
- Detección de conexiones internas hacia IP incluidas en listas

negras.

- Detección de conexiones RDP a equipos internos desde internet.
- Detección de conexiones remotas al cliente desde internet y sin uso de VPN del cliente
- Detección de conexiones remotas desde el cliente hacia internet usando aplicaciones de escritorio remoto.
- Detección de conexiones a posibles archivos compartidos desde fuera del cliente.
- Detección de conexiones a protocolos vulnerables.
- Detección de conexiones desde múltiples fuentes fuera del cliente a un solo destino de la red interna.
- Detección de conexiones internas hacia IP incluidas en listas negras (1er filtro).
- Detección de solicitudes DNS que no se pueden resolver.
- Detección de archivos con contenido malware.
- Detección de ataques de fuerza bruta hacia el protocolo SMB en servidores Windows.
- Detección de ataques de fuerza bruta hacia el protocolo SMB en servidores Linux.
- Detección de escaneos no autorizados hacia la infraestructura de la institución.
- Detección de ataques de directorio transversal hacia aplicaciones web.

El detalle de los casos de uso se muestra en la tabla 7 del ANEXO 08; en lo que respecta a lo posterior de su definición, se configuraron los mismos en la interfaz de grayloc cuyo procedimiento se detalla en el ANEXO 08.

Respecto al procedimiento de gestión de análisis forense la detección y recuperación de evidencias en dispositivos de almacenamiento, teniendo como fin mantener la integridad de la información, se muestran dichos procedimientos en las tablas mostradas en el ANEXO 03 y las ilustración 35 del anexo 08.

3.4.5 Procedimiento de identificación de vulnerabilidades

Respecto al procedimiento de identificación de vulnerabilidades, se detalla en el Anexo 01 del presente informe y los pasos más relevantes son:

- Identificación de las vulnerabilidades de la infraestructura tecnológica a monitorear a partir de fuentes y procesos de detección de vulnerabilidades como : Escaneo de vulnerabilidades realizados por Royal ITC y el cliente, páginas web informativas, boletines especializados de seguridad (ICSPA), otras fuentes de información de vulnerabilidades.
- Registro de las vulnerabilidades y la evidencia en el Sistema de gestión de vulnerabilidades y asignación de responsable del cliente y registro en el estado “Asignado”.
- Informe del plan de acción (dentro de 48 Horas) y una fecha tentativa de solución de la vulnerabilidad y efectuando la actualización en el sistema: “En curso”.
- Solución de la vulnerabilidad, si lo soluciona pasa a actualizar el sistema con la evidencia de la resolución de la vulnerabilidad (Actividad 3.4) y si no soluciona, pasa a una Evaluación (Actividad 3.5) mostrados en el Anexo 01.
- Actualización del estado del ticket a “RESUELTO” y registro de la evidencia de la solución de la vulnerabilidad.
- Evaluación de si la vulnerabilidad es aceptada o mitigada: Si es mitigada (Ir a actividad 3.6), si es aceptada (Ir a Actividad 3.12) mostrados en el Anexo 01.
- Actualización del sistema (Actividad 3.4) cambiando de estado: “MITIGADO” y registro de la evidencia.
- Valida la solución implementada por el cliente: Si la solución es aceptada se cierra el caso (Actividad 3.12), si la solución no es aceptada, es definida como vulnerabilidad observada (Actividad 3.10) mostrados en el Anexo 01.
- Verificación de la resolución de la vulnerabilidad realizando un retest en coordinación con el cliente en los tiempos estimados de corrección (establecidos por el cliente), considerando los siguientes estados de vulnerabilidades registradas:

- Resolución correcta y dentro del periodo de Tiempo de estimado: “CERRADO” (Actividad 3.9) mostrados en el Anexo 01.
- En “OBSERVADO” cuando la solución no es la adecuada (Actividad 3.10).
- Actualización del sistema el cambio de estado a “CERRADO”.
- Actualización del estado en el sistema registrando la observación y si sigue en el mismo estado de OBSERVADO, ir a la Actividad 3.1
- Actualización en el sistema la información de Aceptación del Riesgo y el jefe de Ciberseguridad del mismo hace envío de un correo de aceptación del riesgo.
- Actualización el sistema con el estado: “CERRADO”.
- Elaboración y envío mensualmente al Supervisor del Servicio el informe de seguimiento de vulnerabilidades basado en el estado actual de las vulnerabilidades registradas en el sistema de gestión de vulnerabilidades.
- Revisión el informe de seguimiento de vulnerabilidades: Si el informe no tiene observaciones, envía por correo electrónico el informe al jefe de Proyecto del cliente, en caso de no aprobarse, envía correo electrónico al Supervisor SOC con las observaciones a levantar. Ir a la Actividad 13
- Levantamiento de observaciones y envía nuevamente al Supervisor de Servicio SOC para su aprobación.
- Envío al jefe de Proyecto del CLIENTE el Informe de Seguimiento de Vulnerabilidades

3.4.6 Procedimiento de análisis forense

Respecto al procedimiento de análisis forense, se detalla en el Anexo 01 del presente informe y los pasos más relevantes son:

- Generación de caso mediante el Sistema de Gestión de Tickets (TICKETERA) a Royal ITC, solicitando el análisis forense, completando los campos de la solicitud.
- El Supervisor de Servicio Royal ITC evalúa la aprobación de la

solicitud para asignar el ticket al Analista Forense: Si ¿Aprueba solicitud?, entonces procede a la asignación de la solicitud, si no, al cierre del ticket

- Asigna el ticket al Analista Forense en el Sistema de Gestión de Tickets (TICKETERA) correspondiente al Servicio de Análisis Forense.
- Evaluación del caso con el fin de determinar cómo se realizará la investigación, entre ellas si se debe realizar una visita a las instalaciones del cliente.
- En caso se requiera realizar una visita a las instalaciones del cliente, se coordina mediante el Sistema de Gestión de Tickets (TICKETERA) con el cliente.
- El Analista Forense realiza la visita acompañado por un miembro del personal de Seguridad o quien sea designado por el cliente.
- El cliente otorga permisos mediante una autorización al Analista Forense para recolectar evidencia que contenga información para la investigación.
- En caso se encuentre alguna evidencia, por ejemplo, un disco duro, se generará un hash y se colocará en un formulario. Toda evidencia se retirará en un sobre lacrado para evitar alguna manipulación sobre el mismo.
- Culmina la visita y reporta al cliente el retiro de la evidencia para su análisis.
- En caso la evidencia ha sido enviada por el cliente, el Analista Forense recibe la evidencia y en primera instancia debe examinar que ésta se encuentre asegurado de forma correcta (sellado por calor, cinta precinto, etc.); también se debe consultar que en el formulario se encuentre inscrito el código hash generado para su verificación. En caso de alguna observación, se hace de conocimiento al Supervisor del Servicio para el cierre del ticket.
- Cada vez que la evidencia es retirada de su almacenamiento seguro se actualizará el formulario de cadena de custodia para ese número de caso.

- Cada caso que tenga evidencia física deberá tener un formulario de cadena de custodia generado y almacenado con la evidencia.
- Procede con la copia de la información que se encuentra en el dispositivo de almacenamiento que ha sido registrado como evidencia.
- Se creará un directorio para almacenar las imágenes y los archivos de procesamiento. Al crear una nueva carpeta, el nombre de ésta consistirá solo en el número de caso (ticket).
- Procede con la manipulación de los datos, búsqueda de evidencia y análisis de éstas.
- Cada hallazgo encontrado debe ser correctamente registrado.
- Genera y envía por correo electrónico el informe al Supervisor del Servicio, el cual contiene información sobre las personas involucradas en la investigación, conclusiones u opiniones sobre la evidencia examinada. No se reprimirá, ocultará ni distorsionará ningún incidente.
- Procede con el levantamiento de observaciones y envía nuevamente por correo electrónico al Supervisor del Servicio para su aprobación.

CAPÍTULO IV
CONCLUSIONES

4.1 Justificación

La implementación del servicio de centro de operaciones de ciberseguridad permitirá al cliente contar con mayor seguridad en sus plataformas, además permitirá reducir la vulnerabilidad de la información que considere importante y que implique riesgos si se corrompiera o llegar a perder.

4.2 Presentación de Resultados

Se muestran los resultados obtenidos, en el Anexo 13, gracias a la implementación de servicio de Centro de Operaciones de Ciberseguridad (CyberSoc) con plataformas opensource a una entidad financiera a través del monitoreo de plataformas, gestión de vulnerabilidades, respuestas ante incidentes, gestión y correlación de eventos y gestión de análisis forense; los resultados acerca de los procedimientos antes mencionados se muestran a través de los eventos e incidentes registrados, la gestión de vulnerabilidades desarrollada en el Dashboard, los tiempos de respuesta registrados, la cantidad de eventos por turno durante el mes de mayo del 2021.

Respecto al monitoreo de plataforma, se registraron las alertas según incidente o evento, basándose en cinco estados de PRTG: DOWN, WARNING, UNUSUAL, PAUSED, UNKNOWN y dicha información se registró como ticket o bitácora y dentro del proceso de monitoreo de plataformas se

dio reinicio a los equipos de ban total en un conjunto de 56 equipos distribuidos en 8 grupos, reinicios que se dieron en horarios entre las 8:00 pm a 8:00 am; los registros en estado UNKNOWN se coordinaron para su reporte con un margen de 30 minutos de haberse iniciado el incidente, finalmente todos los registros se compilaron en la bitácora de monitoreo que consideró aspectos como: ITEM, Fecha De Alerta, Hora De Alerta, Fecha De Notificación, Hora De Notificación, Tiempo De Notificación, Fecha De Fin, Hora Fin, Tiempo Solución, Tipo De Alerta, Categoría, Plataforma, Servidor, Ubicación Del Problema – Sensor, Nivel De Criticidad, Turno, Monitor Responsable, Ticket (Sistema Integrado) Royal ITC. Causa De Alerta, Responsable, SLA Incidente, Cumplimiento SLA Incidente, SLA Evento, Cumplimiento SLA Evento y Ruta; tal como muestran los resultados, la mayoría de eventos reportados se resolvieron el mismo día que fueron alertados, respecto al nivel de criticidad de eventos reportados, la mayoría de los eventos fueron categorizados con niveles críticos, tal como se muestra en la tabla del Anexo 07, además la mayoría de eventos e incidentes alertados por la herramienta PRTG fueron de caídas en las diferentes plataformas, también se observaron alertas considerables de eventos e incidentes inusuales, los mismos que debieron ser solucionados en un determinado tiempo; respecto al tiempo de solución de los incidentes el cliente estableció que los mismos debían ser resueltos de acuerdo a su nivel de complejidad y criticidad.

Respecto a la gestión de vulnerabilidades, se obtuvieron un total de 320 vulnerabilidades , para el mes de mayo se obtuvo un total de 320 vulnerabilidades en la fase 1, de los cuales 10 fueron críticas, 5 altas, 21 media, 1 baja y 283 informativas y para el mes de junio, se desarrolló el análisis de vulnerabilidades en 55 servidores, de donde se obtuvo un total de 549 vulnerabilidades en fase 1, de los cuales 9 fueron críticas, 22 altas, 56 media, 1 baja y 461 informativas.

Respecto a la respuesta ante incidentes y al tiempo de respuesta, se evidenció que de un total de 1135 incidentes, 660 (58.15%) incidentes si fueron solucionados a tiempo, 474 incidentes fueron solucionados por fuera del tiempo de resolución y solamente 1 incidente no fue solucionado y al 17 de julio se logró solucionar 38 incidentes y 3 incidentes no fueron solucionados.

Respecto a la gestión y correlación de eventos en promedio los eventos para el mes de mayo fueron 350 durante el turno noche y el número de eventos por nivel criticidad para el mes de mayo fueron un total de 2377, siendo 1419 de nivel crítico,146 de nivel alto, 31 de nivel medio y 781 de nivel bajo. Finalmente respecto a la gestión de análisis forense, no se tuvieron requerimientos asociados al servicio.

4.3 Conclusiones

1. Se logró implementar el servicio centro de operaciones de ciberseguridad (CyberSoC) con plataformas opensource en una entidad financiera, que permitió el monitoreo, detección, análisis, prevención y seguimiento de eventos e incidentes de ciberseguridad en los equipos e instalaciones de la entidad financiera a través del uso de herramientas tecnológicas obteniendo resultados favorables y el cumplimiento de metas establecidas en conjunto con el cliente.
2. Se diseñó la topología necesaria para la implementación del Centro de Operaciones de Ciberseguridad detallando todos los requerimientos necesarios y adaptando nuevas soluciones a las limitantes presentadas.
3. Se diseñó e implementó la plataforma de gestión de alertas de servidores a través de la integración de herramientas informáticas tanto en los servidores del cliente y de la empresa proveedora.
4. Se diseñar e implementó la plataforma de alertas de seguridad a la que tanto el proveedor como el cliente tuvieron acceso.
5. Se establecieron procedimientos para la respuesta ante incidencias de seguridad, reportes, reportes de inteligencia de amenazas, análisis forense y gestión de vulnerabilidades tanto para el cliente como para la empresa con el fin de mejorar la capacidad de respuesta de ambas partes.

CAPÍTULO V
RECOMENDACIONES

1. Se recomienda tener en cuenta posteriormente el uso y la adaptabilidad de la herramienta Graylog para la gestión y correlación de eventos en entidades financieras.

BIBLIOGRAFIA

AGESIC. (2022). Guía Gestión de vulnerabilidades .

Avenía, C. (2017). Fundamentos de seguridad informática . Bogotá, Colombia: Fondo editorial Areandino.

Barrera, D., Dorvigny, D., & Montesino, R. (2021). Plataforma de inteligencia de amenazas la Red Nacional Universitaria .

Blanco, J. (2017). *Cyberinteligencia, la vía para la ciberseguridad.* Obtenido de https://gcivil.orex.es/local_repository/koha_upload/6a7214531a3239c800669262ea3d0b36_1%20CIBERINTELIGENCIA,%20LA%20V%C3%8DA%20PARA%20LA%20CIBERSEGURIDAD.pdf

Ciberseguridad . (2022). *Ciberseguridad*. Obtenido de https://ciberseguridad.com/guias/prevencion-proteccion/inteligencia-amenazas/

EY. (2022). ¿La ciberseguridad solo se convierte en una prioridad una vez que has sido atacado? *Execution*, 30.

Kapersky Lab . (2017). Centro de operaciones de seguridad con tecnología Kapersky Lab. 22.

López, M. (2007). Análisis forense digital.

ManageEngine. (2021). Usar Indicadores para enfrentar los ataques a la seguridad .

Martínez, M. (2021). Implementación de un centro de operaciones de seguridad (SOC) de código abierto con elementos de red para sistemas industriales .

Miró, F. (2012). El cibercrimen.

Morales, C., Moreno, O., & Ortigoza, J. (2014). Propuesta de un modelo de centro de operaciones de seguridad (SOC) para fuerza aérea colombiana.

NEOSECURE. (2022). *NEOSECURE*. Obtenido de https://ciberseguridad.neosecure.com/blog/monitoreo-y-deteccion-cuando-la-prevencion-falla

OEA. (2019). Un abordaje integral de la ciberseguridad .

Ormachea, J. F. (2020). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. doi:https://orcid.org/0000-0002-9119-8846

Ponce, J. (2021). Indicadores de compromiso (IoC) para detección de amenazas en la seguridad informática con enfoque al código malicioso.

Ríos, L. (2021). *ESIC*. Obtenido de https://www.esic.edu/rethink/tecnologia/seguridad-pasiva-y-activa-en-informatica

Roa, J. F. (2013). Seguridad Informática . Mc Graw Hill Education .

Tenable. (2022). *tenable*. Obtenido de https://es-la.tenable.com/source/vulnerability-management#:~:text=La%20gesti%C3%B3n%20de%20vulnerabilidades%20es,organizaci%C3%B3n%20contra%20la%20Cyber%20Exposure.

Valdez, A. (2009). El cibercrimen.

ANEXOS

Anexo 01: Detalle de procedimientos de identificación de vulnerabilidades

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	Identificación de vulnerabilidades	Identifica las vulnerabilidades de la infraestructura tecnológica a monitorear a partir de las siguientes fuentes y procesos de detección de vulnerabilidades: Escaneo de vulnerabilidades realizados por Royal ITC y el cliente Páginas web informativas Boletines especializados de seguridad (ICSPA) Otras fuentes de información de	Gestor de Vulnerabilidades (Royal ITC)	Correos recibidos Informes de Escaneo de vulnerabilidades y Ethical Hacking Otros

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		vulnerabilidades.		
2	Realizar Seguimiento de las vulnerabilidades			
2.1	Registro en el Sistema	Registra las vulnerabilidades y la evidencia en el Sistema de gestión de vulnerabilidades. Se asigna al responsable del cliente y se registra el estado en "Asignado".	Operador SOC (Royal ITC)	Registro de vulnerabilidades ingresadas en el sistema de gestión de vulnerabilidades
2.2	Plan de acción	Informa del plan de acción (dentro de 48 Horas) y una fecha tentativa de solución de la vulnerabilidad y efectuando la actualización	Cliente	Correo electrónico Informe de Plan de acción

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		en el sistema: “En curso”.		
2.3	Solución	Soluciona la vulnerabilidad si lo soluciona pasa a actualizar el sistema con la evidencia de la resolución de la vulnerabilidad (Actividad 3.4) y si no soluciona, pasa a una Evaluación (Actividad 3.5)	Cliente	Ninguno
2.4	Actualizar el Sistema registrando la evidencia	Actualiza el estado del ticket a “RESUELTO” y registra la evidencia de la solución de la vulnerabilidad.	Cliente	Evidencia de la resolución

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
2.5	Evaluación	Evalúa si la vulnerabilidad es aceptada o mitigada: Si es mitigada (Ir a actividad 3.6) Si es aceptada (Ir a Actividad 3.12)	Cliente	Ninguno
2.6	Mitigación	Actualiza el sistema (Actividad 3.4) cambiando de estado: "MITIGADO" y se registra la evidencia.	Cliente	Registro y actualización
2.7	Validar Mitigación	Valida la solución implementada por el cliente: Si la solución es aceptada se cierra el caso (Actividad 3.12) Si la solución no es aceptada, es definida como vulnerabilidad	Gestor de vulnerabilidades (Royal ITC)	Ninguno

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		observada (Actividad 3.10)		
2.8	Verificación de Resolución de vulnerabilidades	Verifica la resolución de la vulnerabilidad realizando un retest en coordinación con el cliente en los tiempos estimados de corrección (establecidos por el cliente), considerando los siguientes estados de vulnerabilidades registradas: Resolución correcta y dentro del periodo de Tiempo de estimado: “CERRADO” (Actividad 3.9) En “OBSERVADO”	Gestor de vulnerabilidades (Royal ITC)	Registro de ingreso al sistema de registro de vulnerabilidades

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		cuando la solución no es la adecuada (Actividad 3.10).		
2.9	Aceptación de la solución	Actualiza en el sistema el cambio de estado a "CERRADO".	Operador SOC Gestor de vulnerabilidades (Royal ITC)	Actualización en el sistema
3.1	Vulnerabilidad observada	Actualiza el estado en el sistema registrando la observación y si sigue en el mismo estado de OBSERVADO, ir a la Actividad 3.1	Operador SOC Gestor de vulnerabilidades (Royal ITC)	Actualización en el sistema
3.2	Vulnerabilidad Aceptada	Actualiza en el sistema la información de	Cliente	Actualización en el sistema

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		Aceptación del Riesgo y el jefe de Ciberseguridad del mismo hace envío de un correo de aceptación del riesgo.		Correo de información
3.3	Cerrar	Actualiza el sistema con el estado: "CERRADO".	OPERADOR SOC (Royal ITC)	Actualización en el sistema
3.4	Elaboración de informe	Elabora y envía mensualmente al Supervisor del Servicio el informe de seguimiento de vulnerabilidades basado en el estado actual de las vulnerabilidades registradas en el sistema de gestión de vulnerabilidades.	Supervisor SOC (Royal ITC)	Correo electrónico adjuntando el Informe de Seguimiento de vulnerabilidades

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
3.5	Aprobación del informe	Revisa el informe de seguimiento de vulnerabilidades: Si el informe no tiene observaciones, envía por correo electrónico el informe al jefe de Proyecto del cliente. En caso de no aprobarse, envía correo electrónico al Supervisor SOC con las observaciones a levantar. Ir a la Actividad 13	Supervisor del servicio SOC (Royal ITC)	Correo electrónico de envío del informe al CLIENTE o al Supervisor SOC según corresponda
3.6	Corrección de informe	Procede con el levantamiento de observaciones y envía nuevamente al Supervisor de Servicio SOC	Supervisor SOC (Royal ITC)	Correo electrónico de envío del informe de seguimiento de vulnerabilidades

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		para su aprobación.		
3.7	Envío final	Envía al jefe de Proyecto del CLIENTE el Informe de Seguimiento de Vulnerabilidades	Supervisor de servicio SOC (Royal ITC)	Correo electrónico de envío del Informe de Seguimiento de Vulnerabilidades

Fuente: (Royal ITC,2021)

Tabla 5 Procedimiento de identificación de vulnerabilidades – cliente

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	Identificación de vulnerabilidades	Identifica las vulnerabilidades de la infraestructura tecnológica a monitorear alcanzando un Registro de evidencia.	Cliente (Analista de seguridad informática)	Correo enviado Registro de evidencia Otros
2	Registro de vulnerabilidades			
2.1	Envío de Identificación de vulnerabilidades	Envía un correo con la Evidencia de la identificación de las	Cliente	Correo electrónico Archivo cifrado

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		vulnerabilidades en un archivo cifrado (El password se envía por otro medio de comunicación).		
2.2	Registro en el Sistema	Se registra en el sistema de gestión de vulnerabilidades la información recibida por parte del cliente y asigna al responsable del activo para la solución de la vulnerabilidad. Estado "Asignado"	OPERADOR SOC	Registro en el sistema Correo electrónico
3	Seguimiento de las vulnerabilidades (Cliente)			
3.1	Plan de acción	Informa del plan de acción (dentro de 48 Horas) con la fecha tentativa de solución actualizando en el Sistema como:" En curso".	Cliente	Registro en el sistema Correo Electrónico

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
3.2	Envío de la evidencia con la Resolución de la vulnerabilidad	Envía un correo con la Evidencia de la Resolución de las vulnerabilidades en un archivo cifrado (El password se envía por otro medio de comunicación).	Cliente	Correo electrónico Archivo cifrado
3.3	Cerrar	Actualiza el sistema con el estado: CERRADO.	OPERADOR SOC (Royal ITC)	Actualización en el sistema

Fuente: (Royal ITC,2021

Anexo 02: Detalle de procedimientos de identificación de vulnerabilidades

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	Recibir notificaciones de eventos	Mediante correo electrónico el Operador SOC recibe notificaciones de eventos desde la herramienta de correlación de eventos.	OPERADOR SOC	Correo Electrónico de la herramienta de correlación de eventos (**Ver Anexo 01**)
2	Analizar evento	Realiza el análisis para descartar si es o no un incidente de seguridad. ¿Es un incidente de seguridad? **Sí** → Registrar incidente de seguridad (Actividad N°3) **No** → Fin del proceso	OPERADOR SOC	-
3	Registrar incidente de seguridad	Registra el incidente en el Sistema de Gestión de Tickets y en la bitácora de incidentes de	OPERADOR SOC	Sistema de Gestión de Tickets (**Ver Anexo 02**)

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		seguridad. **Estado de ticket: nuevo**		Bitácora de incidentes de seguridad (**Ver Anexo 03**)
4	Asignar y notificar al responsable del activo	Asigna y hace conocimiento sobre el incidente al responsable del activo, indicando que se está elaborando las acciones de respuesta recomendadas. **Estado de ticket: en curso (asignado)**	OPERADOR SOC	Sistema de Gestión de Tickets
5	Recibir notificación del incidente de seguridad	Toma conocimiento sobre el incidente de seguridad. **Estado de ticket: en curso (planificado)**	RESPONSABLE DEL ACTIVO (Cliente)	Sistema de Gestión de Tickets
6	Escalar incidente de seguridad	Escala el incidente al Analista de seguridad para el análisis.	OPERADOR SOC	Correo electrónico

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
7	Analizar incidente de seguridad	Recolecta información indispensable para identificar porqué se originó el incidente. ¿El incidente es crítico? **Sí** → Convocar reunión con el CSIRT (Actividad N°8) **No** → Proponer Acciones de Respuesta (Actividad N°10)	ANALISTA DE SEGURIDAD	-
8	Convocar reunión con el CSIRT	Ante un incidente crítico, que debe ser tratado con rapidez, se convoca al Equipo de respuesta ante incidentes – CSIRT.	ANALISTA DE SEGURIDAD	-
9	Evaluar respuestas ante el incidente	Formulan estrategias para hacer frente al incidente y minimizar el	CSIRT	-

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		impacto.		
10	Proponer Acciones de Respuesta	Elabora una serie de acciones de respuesta recomendadas para lograr contener, erradicar incidente y responder incidente.	ANALISTA DE SEGURIDAD CSIRT	Acciones de Respuesta
11	Ejecutar Acciones de Respuesta	Pone en marcha las acciones de respuesta recomendadas por el SOC. ¿Se logró resolver el incidente? **Sí** → Cerrar incidente (Actividad N°14) **No** → Reportar al SOC (Actividad N°12)	RESPONSABLE DEL ACTIVO (Cliente)	Acciones de Respuesta
12	Reportar al SOC	Informa que no se ha logrado controlar el	RESPONSABLE DEL ACTIVO (Cliente)	Correo electrónico

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		incidente, por lo solicita asistencia al SOC.		
13	Registrar notificación del responsable	Registra toda notificación que envíe el responsable del Activo en caso requiera asistencia.	OPERADOR SOC	Sistema de Gestión de Tickets
14	Cerrar incidente	Cierra el ticket que corresponde al incidente de seguridad, indicando que fue superado. **Estado de ticket: resuelto**	RESPONSABLE DEL ACTIVO (Cliente)	Sistema de Gestión de Tickets
15	Presentar Informe	Elabora un informe con el balance general del servicio. La información descrita en el informe corresponde a lo consignado en el SLA.	SUPERVISOR SOC	Informe

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
16	Aprobar Informe	El supervisor de servicio verifica el documento y si el informe no tiene observaciones, se envía el documento al cliente. ¿Aprueba el informe? **Sí** → Entregar informe al cliente (Actividad N°18) **No** → Corregir informe (Actividad N°1)	SUPERVISOR DEL SERVICIO	Informe
17	Corregir Informe	Procede con el levantamiento de observaciones en el informe y presenta nuevamente al Supervisor del Servicio para su firma de aprobación.	SUPERVISOR SOC	Informe
18	Entregar Informe al cliente	Se envía el informe al Jefe de Proyecto	SUPERVISOR DEL SERVICIO	Informe

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		mediante correo electrónico.		

Tabla 6 Procedimiento de gestión y respuesta incidentes de seguridad de TI

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	Monitorear eventos	El operador SOC supervisa las alarmas notificadas por la herramienta de monitorización de infraestructura.	OPERADOR SOC	Notificaciones de la Herramienta de Monitorización de Infraestructura
2	Descartar eventos	Determina si el evento corresponde a un incidente de TI; además debe verificar que el activo se encuentra dentro del alcance entregado por el cliente. ¿Es un incidente de TI? **Sí** → Registrar incidente de TI (Actividad N°3) **No** → Fin de la actividad	OPERADOR SOC	Lista de activos

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
3	Registrar incidente de TI	Registra el incidente en el Sistema de Gestión de Tickets y en la bitácora de incidentes de TI. **Estado de ticket: nuevo**	OPERADOR SOC	Bitácora de incidentes de TI (**Ver Anexo 04**) Sistema de Gestión de Tickets
4	Asignar y notificar incidente de TI al responsable	Asigna y hace conocimiento sobre el incidente al responsable del activo. **Estado de ticket: en curso (asignado)**	OPERADOR SOC	Sistema de Gestión de Tickets
5	Validar incidente	Verifica que el ticket cuente con la información completa y que corresponda a un incidente de seguridad de TI.	RESPONSABLE DEL ACTIVO (Cliente)	Sistema de Gestión de Tickets
6	Ejecutar medidas correctivas	Pone en marcha las medidas correctivas. Estas medidas correctivas deben frenar el impacto ocasionado sobre el flujo de los procesos involucrados.	RESPONSABLE DEL ACTIVO (Cliente)	-
7	Solucionar el incidente	Realiza las pruebas necesarias para establecer que no hay secuelas u otros	RESPONSABLE DEL ACTIVO (Cliente)	-

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		incidentes que se puedan asociar posteriormente.		
8	Resolver incidente	Cierra el ticket que corresponde al incidente de TI, indicando que se superó el incidente. **Estado de ticket: resuelto**	RESPONSABLE DEL ACTIVO (Cliente)	Sistema de Gestión de Tickets
9	Validar si incidente ha sido solucionado	Verifica que el incidente se encuentre solucionado, revisando la herramienta de monitorización. ¿Se solucionó incidente? **Sí** → Fin de la actividad **No** → Asignar y notificar incidente de TI al responsable (Actividad N°4)	OPERADOR SOC	Herramienta de Monitorización de Infraestructura
10	Elaborar reporte de incidentes de TI	Elabora el reporte de incidentes de TI con la finalidad de recopilar información para documentar lecciones aprendidas.	OPERADOR SOC	Reporte de incidentes de TI
11	Revisar reporte	Verifica que el reporte cuente con la información que será presentado al cliente.	SUPERVISOR SOC	Reporte

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
12	Aprobar reporte	Da conformidad al reporte para enviarlo al cliente.	SUPERVISOR DEL SERVICIO	Reporte
13	Entregar reporte al cliente	Se envía el reporte al Jefe de Proyecto mediante correo electrónico.	SUPERVISOR DEL SERVICIO	Reporte

Anexo 03: Detalle de procedimientos de análisis forense

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	Creación de ticket	Genera un caso mediante el Sistema de Gestión de Tickets (TICKETERA) a Royal ITC, solicitando el análisis forense, completando los campos de la solicitud. **Estado de ticket: nuevo**	Cliente	Generación de la solicitud **(ANEXO 1)**
2	Evaluación de la solicitud	El Supervisor de Servicio Royal ITC evalúa la aprobación de la solicitud para asignar el ticket al Analista Forense.	SUPERVISOR DEL SERVICIO	Aprobación de la solicitud **(ANEXO 2)**

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		¿Aprueba solicitud? **Sí** → Asignación de la solicitud (Actividad N°3) **No** → Cierre del ticket (Actividad N°18)		
3	Asignación de la solicitud	Asigna el ticket al Analista Forense en el Sistema de Gestión de Tickets (TICKETERA) correspondiente al Servicio de Análisis Forense. **Estado de ticket: en curso (asignado)**	SUPERVISOR DEL SERVICIO	Actualizar el Ticket en curso (asignado) en el Sistema de Gestión de Tickets
4	Análisis del caso	Evalúa el caso con el fin de determinar cómo se realizará la investigación, entre ellas si se debe realizar una visita a las instalaciones del cliente.	ANALISTA FORENSE	Actualizar estado del Ticket en curso (planificado) en el Sistema de Gestión de Tickets (TICKETERA)

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		¿Se requiere visita? **Sí** → Coordinación de visita (Actividad N°5) **No** → Recepción de la evidencia (Actividad N°10) **Estado de ticket: en curso (planificado)**		
5	Coordinación de visita	En caso se requiera realizar una visita a las instalaciones del cliente, se coordina mediante el Sistema de Gestión de Tickets (TICKETERA) con el cliente.	ANALISTA FORENSE	Registro de la coordinación en el Sistema de Gestión de Tickets (TICKETERA)
6	Visita al cliente	El Analista Forense realiza la visita acompañado por	ANALISTA FORENSE	Copia o foto de registro de visitas del cliente

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		un miembro del personal de Seguridad o quien sea designado por el cliente.		(Entrada)
7	Recolección de información	El cliente otorga permisos mediante una autorización al Analista Forense para recolectar evidencia que contenga información para la investigación. ¿Se encontraron evidencias? **Sí** → Retiro de evidencias (Actividad N°8) **No** → Termino de la visita (Actividad N°9)	ANALISTA FORENSE	Autorización de recolección de información **(ANEXO 3)**

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
8	Retiro de evidencias	En caso se encuentre alguna evidencia, por ejemplo, un disco duro, se generará un hash y se colocará en un formulario. Toda evidencia se retirará en un sobre lacrado para evitar alguna manipulación sobre el mismo.	ANALISTA FORENSE	Formulario de registro de evidencia **(ANEXO 4)**
9	Término de la visita	Culmina la visita y reporta al cliente el retiro de la evidencia para su análisis.	ANALISTA FORENSE	Copia o foto de registro de visitas del cliente (Salida)

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
10	Recepción de la evidencia	En caso la evidencia ha sido enviada por el cliente, el Analista Forense recibe la evidencia y en primera instancia debe examinar que ésta se encuentre asegurado de forma correcta (sellado por calor, cinta precinto, etc.); también se debe consultar que en el formulario se encuentre inscrito el código hash generado para su verificación. En caso de alguna observación, se hace de conocimiento al Supervisor del Servicio para el cierre del ticket.	ANALISTA FORENSE	Formulario de registro de evidencia **(ANEXO 4)**

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		¿Existe alguna observación? **Sí** → Cierre del ticket (Actividad N°18) **No** → Extracción de la evidencia (Actividad N°11)		
11	Extracción de la evidencia	Cada vez que la evidencia es retirada de su almacenamiento seguro se actualizará el formulario de cadena de custodia para ese número de caso. Cada caso que tenga evidencia física deberá tener un formulario de cadena de custodia generado y	ANALISTA FORENSE	Formulario de Cadena de Custodia **(ANEXO 5)**

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		almacenado con la evidencia.		
12	Preservación de la información	Procede con la copia de la información que se encuentra en el dispositivo de almacenamiento que ha sido registrado como evidencia. Se creará un directorio para almacenar las imágenes y los archivos de procesamiento. Al crear una nueva carpeta, el nombre de ésta consistirá solo en el número de caso (ticket).	ANALISTA FORENSE	Copia de información de la evidencia en un directorio de almacenamiento
13	Análisis de la información	Procede con la manipulación de los datos, búsqueda de	ANALISTA FORENSE	Registro de hallazgos **(ANEXO 6)**

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
		evidencia y análisis de éstas. Cada hallazgo encontrado debe ser correctamente registrado.		
14	Presentación del informe	Genera y envía por correo electrónico el informe al Supervisor del Servicio, el cual contiene información sobre las personas involucradas en la investigación, conclusiones u opiniones sobre la evidencia examinada. No se reprimirá, ocultará ni distorsionará ningún incidente.	ANALISTA FORENSE	Estructura del Informe **(ANEXO 7)** Correo electrónico

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
15	Aprobación del informe	Revisa el informe del análisis forense. ¿Aprueba el informe? **Sí** → Entrega del informe (Actividad N°16) **No** → Corrección del informe (Actividad N°17)	SUPERVISOR DEL SERVICIO	Correo electrónico de aprobación
16	Entrega del informe	Envía el informe al Jefe de Proyecto mediante correo electrónico. ¿Cliente aprueba informe? **Sí** → Resolución del ticket (Actividad N°19) **No** → Corrección del informe (Actividad N°17)	SUPERVISOR DEL SERVICIO	Correo electrónico

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
17	Corrección del informe	Procede con el levantamiento de observaciones y envía nuevamente por correo electrónico al Supervisor del Servicio para su aprobación.	ANALISTA FORENSE	Correo electrónico
18	Cierre del ticket	Procede con esta actividad ante dos posibles situaciones: • El Supervisor del Servicio no aprueba la solicitud. • El Analista Forense encuentra alguna observación durante la extracción de la evidencia. **Estado de ticket: cerrado**	SUPERVISOR DEL SERVICIO	Registro de Ticket cerrado en el Sistema de Gestión de Tickets (TICKETERA)
19	Resolución del ticket	Procede con el cierre del ticket. **Estado de ticket: resuelto**	ANALISTA FORENSE	Actualizar el Ticket resuelto en el Sistema de Gestión de

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
				Tickets (TICKETERA)

Anexo 04: Detalle de registros de incidentes y eventos en mayo 2021

DÍA	INCIDENTE	EVENTOS	TOTAL
01/05/2021 - 02/05/2021	105	190	295
Sábado	53	110	163
Domingo	52	80	132
03/05/2021 - 09/05/2021	300	615	915
Lunes	46	67	113
Martes	37	112	149
Miércoles	41	54	95
Jueves	35	104	139
Viernes	39	156	195
Sábado	37	61	98
Domingo	65	61	126
10/05/2021 - 16/05/2021	260	477	737
Lunes	2	32	34
Martes	35	95	130
Miércoles	35	62	97
Jueves	32	78	110
Viernes	62	74	136
Sábado	59	86	145
Domingo	35	50	85
17/05/2021 - 23/05/2021	241	478	719
Lunes	3	26	29
Martes	65	88	153
Miércoles	35	71	106
Jueves	8	75	83
Viernes	63	89	152
Sábado	3	69	72
Domingo	64	60	124
24/05/2021 - 30/05/2021	199	556	755
Lunes	10	126	136
Martes	31	45	76
Miércoles	62	115	177

Jueves	0	44	44
Viernes	60	84	144
Sábado	4	79	83
Domingo	32	61	95
31/05/2021	30	61	91
Lunes	30	61	91
Total	1135	2337	3512

Anexo 05: Detalle de incidentes y eventos resueltos durante mayo 2021

Fechas de Alerta	Fecha de Alerta	Día	Incidente	Evento	Total	% Resueltos
01/05/2021-	1/05/2021	sáb.	53	110	163	100%
02/05/2021	2/05/2021	dom.	52	80	132	100%
	3/05/2021	lun.	46	59	105	93%
	4/05/2021	mar.	37	105	142	95%
	5/05/2021	mié.	41	53	94	99%
03/05/2021-	6/05/2021	jue.	35	104	139	100%
09/05/2021	7/05/2021	vie.	39	154	193	99%
	8/05/2021	sáb.	37	61	98	100%
	9/05/2021	dom.	65	52	117	93%
	10/05/2021	lun.	2	32	34	100%
	11/05/2021	mar.	35	95	130	100%
	12/05/2021	mié.	35	62	97	100%
10/05/2021-	13/05/2021	jue.	32	77	109	99%
16/05/2021	14/05/2021	vie.	62	74	136	100%
	15/05/2021	sáb.	59	86	145	100%
	16/05/2021	dom.	35	50	85	100%
	17/05/2021	lun.	3	26	29	100%
	18/05/2021	mar.	65	87	152	99%
	19/05/2021	mié.	35	69	104	98%
17/05/2021-	20/05/2021	jue.	8	72	80	96%
23/05/2021	21/05/2021	vie.	63	89	152	100%
	22/05/2021	sáb.	3	68	71	99%
	23/05/2021	dom.	64	60	124	100%
	24/05/2021	lun.	10	126	136	100%
	25/05/2021	mar.	31	43	74	97%
	26/05/2021	mié.	62	115	177	100%
24/05/2021-	27/05/2021	jue.	0	43	43	98%
30/05/2021	28/05/2021	vie.	60	83	143	99%
	29/05/2021	sáb.	3	79	82	99%
	30/05/2021	dom.	32	62	94	99%

31/05/2021	31/05/2021	lun.	30	53	83	91%
Total			1134	2329	3463	99%

Anexo 06: Detalle de incidentes por nivel de criticidad

Semana	Crítico	Alta	Media	Baja	Total
01/05/2021-02/05/2021	102	2	0	1	105
03/05/2021-09/05/2021	274	13	0	13	300
10/05/2021-16/05/2021	252	6	2	0	260
17/05/2021-23/05/2021	229	11	1	0	241
24/05/2021-30/05/2021	195	1	3	0	199
31/05/2021	30	0	0	0	30
Total	1082	33	6	14	1135

Anexo 07: Detalle de eventos por nivel de criticidad

Semana	Crítico	Alta	Media	Baja	Total
01/05/2021-02/05/2021	130	16	0	44	190
03/05/2021-09/05/2021	373	26	7	209	615
10/05/2021-16/05/2021	303	28	4	142	477
17/05/2021-23/05/2021	271	39	7	161	478
24/05/2021-30/05/2021	310	32	11	203	556
31/05/2021	32	5	2	22	61
Total	1419	146	31	781	2377

Anexo 08: Procedimiento de implementación

Procedimiento monitoreo de plataforma

A solicitud del cliente el monitoreo se realizó con la herramienta PRTG. Es importante mencionar que Royal ITC cuenta con una infraestructura de monitoreo basada en Zabbix y otras herramientas establecidas y con personal especializado en dichas herramientas que puede brindar un soporte al sistema ante cualquier eventualidad sin embargo la integración de la herramienta Zabbix y PRTG. La empresa Royal ITC realizó el monitoreo considerando la configuración establecida el cliente sin realizarle ningún cambio. El monitoreo se realizó mediante la conexión VPN desde la infraestructura SERVICIO CLOUD hacia el PRTG, para el cual el cliente entregó un usuario y password para otorgar acceso a Royal ITC. Para iniciar el monitoreo del PRTG, el cliente proporcionó a Royal ITC la configuración de la arquitectura del servidor PRTG y el estado actual de la configuración del PRTG como parte del levantamiento de información hacia Royal ITC. El cliente para poder acceder al sistema de gestión de tickets debía realizarlo con las credenciales generadas por Royal y acceder a través de la conexión VPN.

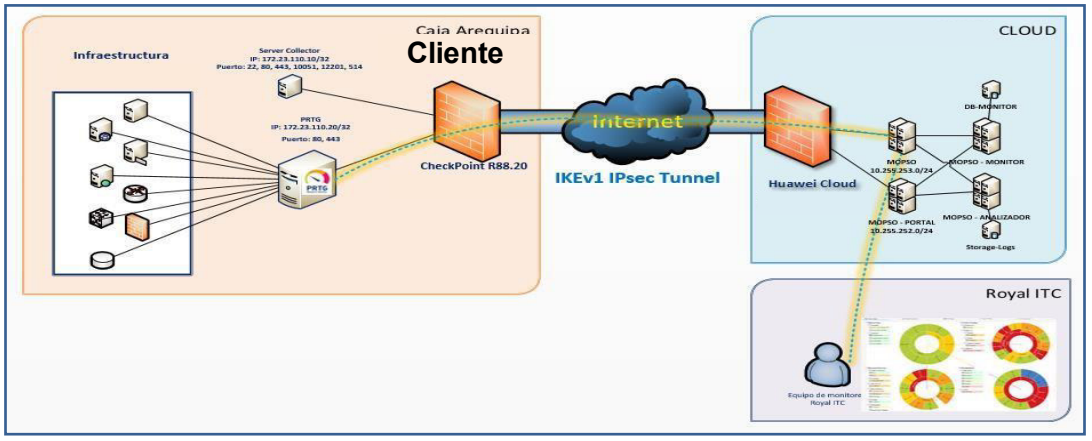

Figura 18 Diagrama de conexión PRTG-SERVICIO CLOUD para monitoreo de plataforma

Fuente: (Royal ITC,2021)

Procedimiento de Gestión de vulnerabilidades

Se realizó la gestión de vulnerabilidades que pudieran ser descubiertas como parte del servicio SOC, se formularon planes de acción tanto para el proveedor y para el cliente para el correcto desarrollo del procedimiento, se muestran dichos planes en las tablas mostradas en el ANEXO 01 y en las siguientes figuras.

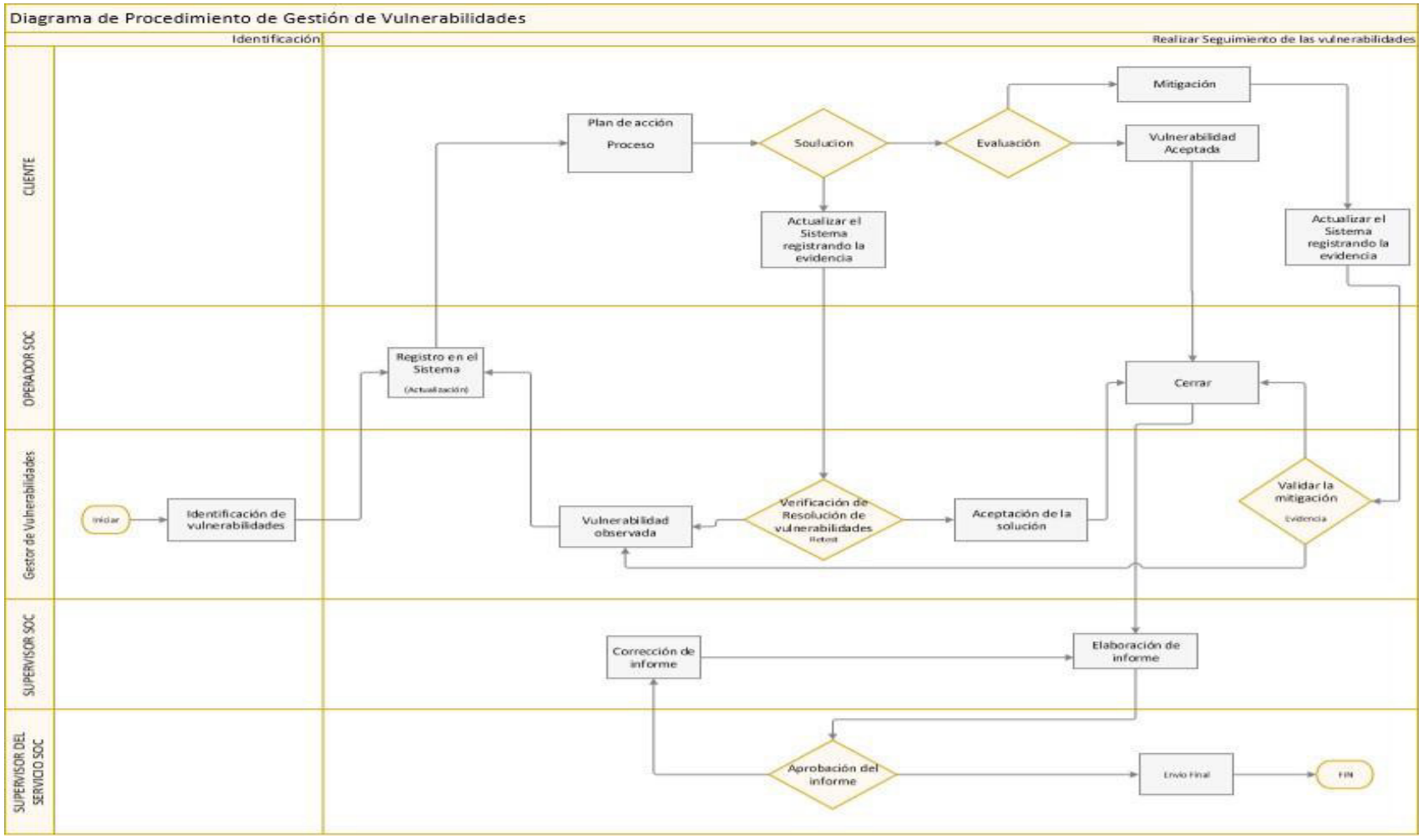

Figura 19 Diagrama de procedimiento de Gestión de Vulnerabilidades- Proveedor

Fuente: (Royal ITC,2021)

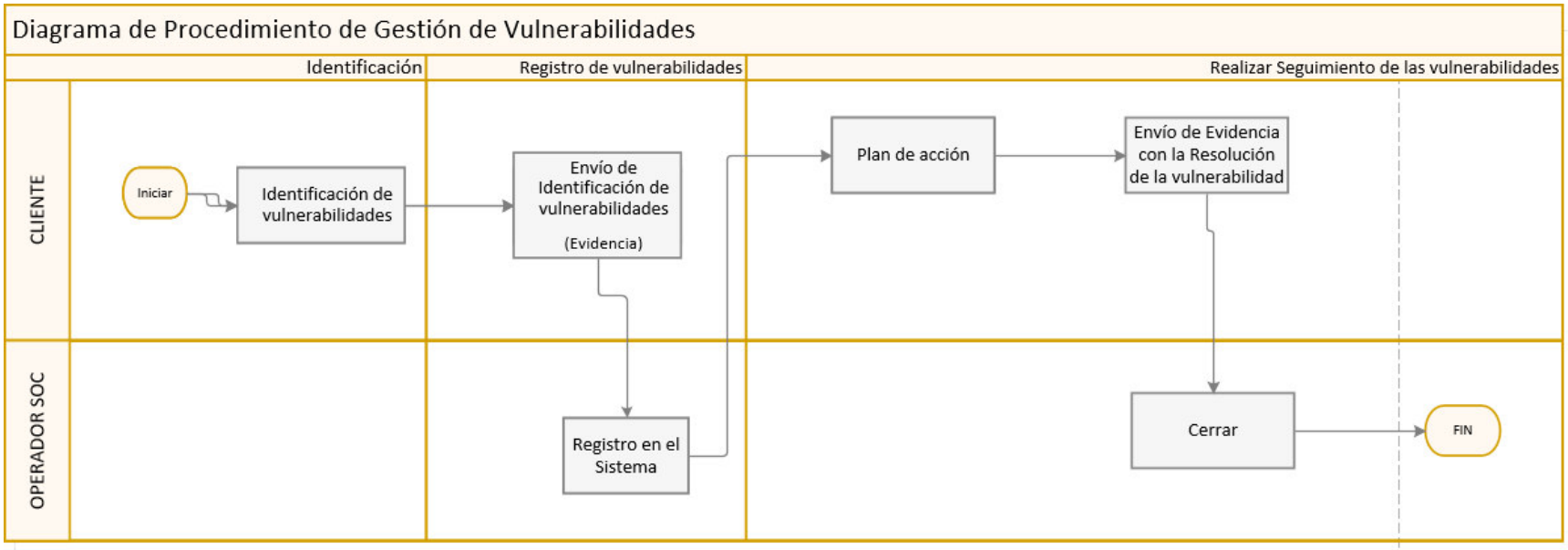

Figura 20 Diagrama de procedimiento de Gestión de Vulnerabilidades- Cliente

Fuente: (Royal ITC,2021)

Procedimiento de respuesta ante incidentes

Se establecieron metodologías para que el cliente pueda tener el conocimiento para reportar y generar oportunamente los incidentes que se relacionaran con los activos de seguridad de la información y activos de TI, se muestran dichos procedimientos en las tablas mostradas en el ANEXO 02 y en las siguientes figuras.

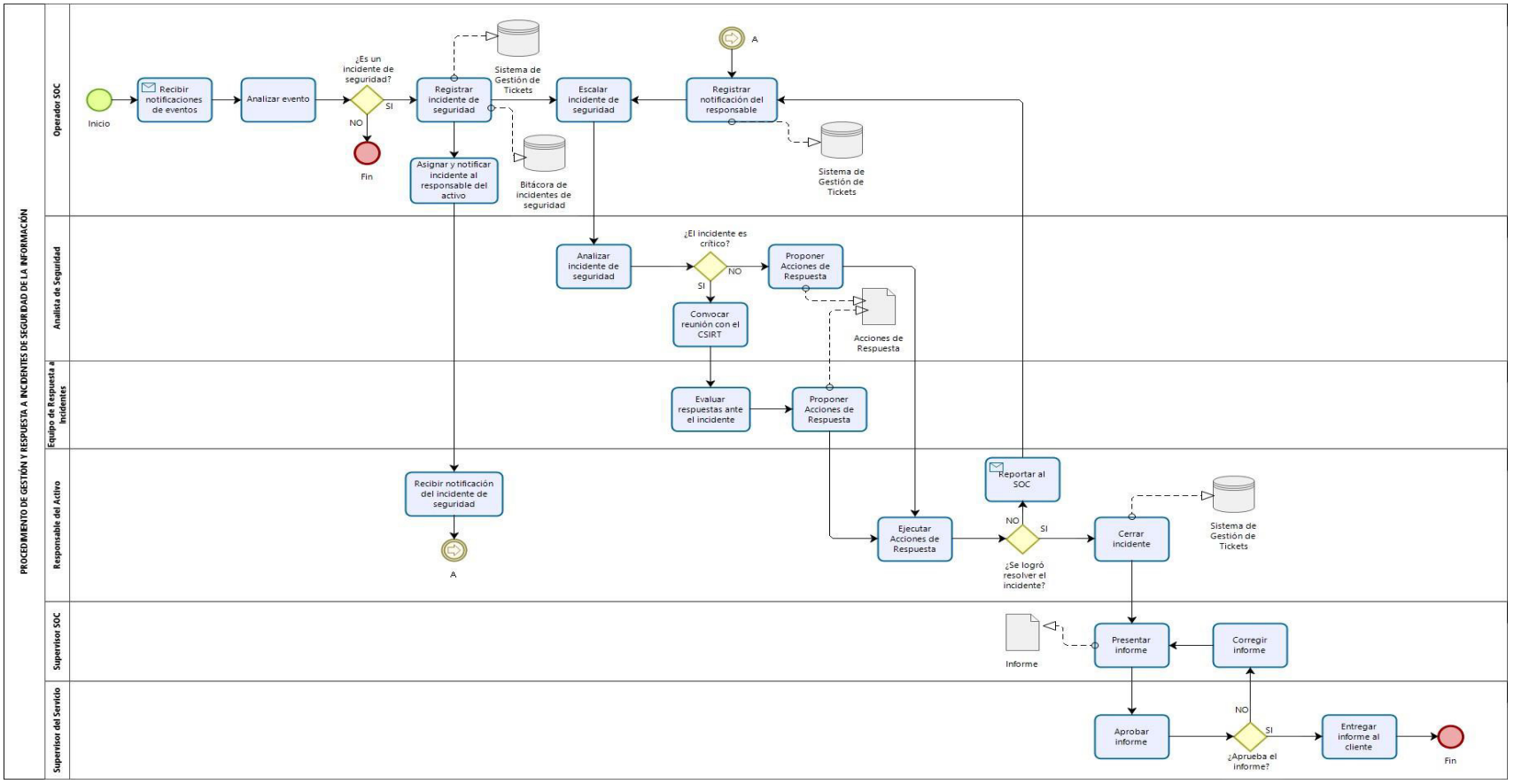

Figura 21 Diagrama de procedimiento de Gestión y Respuesta ante incidentes de seguridad de la información

Fuente: (Royal ITC,2021)

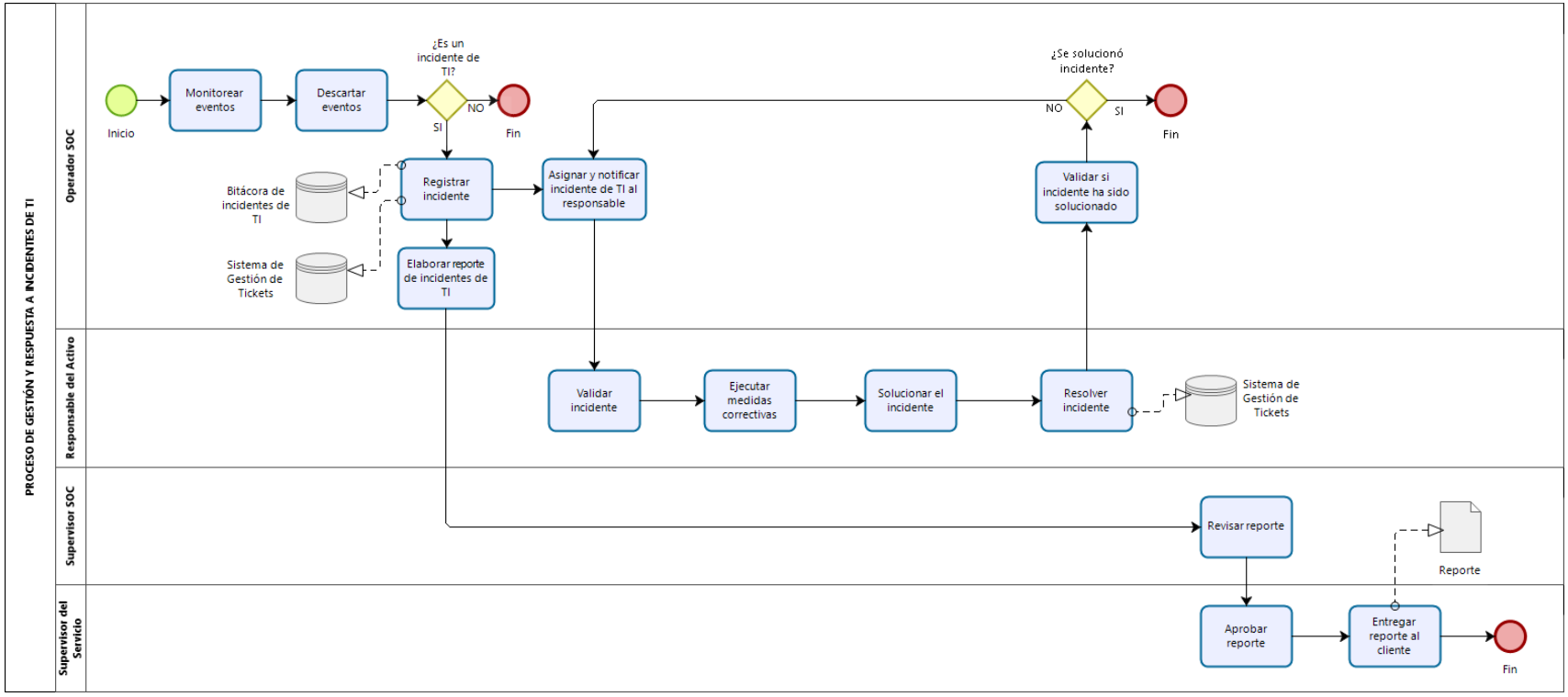

Figura 22 Diagrama de procedimiento de Gestión y Respuesta ante incidentes de seguridad de TI

Fuente: (Royal ITC,2021)

Procedimiento de gestión y correlación de eventos

El primer paso para la configuración y posterior uso de graylog, fue el establecimiento de casos de uso que se muestran en la siguiente tabla.

Tabla 7 Casos de uso

ID	Caso de uso	Objetivo del control
FW-101	Detección de conexiones entrantes al cliente desde fuera de Perú	Identificar los accesos de cuentas de dominio que provengan de otros países
FW-102	Detección de conexiones internas hacia IP incluidas en listas negras	Identificar conexiones de IP internas a direcciones IP consideradas maliciosas
FW-103	Detección de conexiones RDP a equipos internos desde Internet	Identificar sesiones RDP abiertas desde Internet hacia equipos internos
FW-104	Detección de conexiones remotas al cliente desde Internet y sin uso de VPN del cliente	Identificar conexiones abiertas desde Internet hacia equipos internos
FW-104-1	Detección de conexiones remotas desde el cliente hacia Internet usando aplicaciones de escritorio remoto	Identificar usuarios no permitidos del cliente que realizan conexiones de escritorio remoto hacia Internet utilizando aplicaciones de escritorio remoto
FW-105	Detección de conexiones a posibles archivos compartidos desde fuera del cliente	Identificar conexiones TCP 445 SMB desde Internet a equipos internos
FW-107	Detección de conexiones a protocolos vulnerables	Identificar sesiones abiertas desde equipos externos hacia protocolos considerados vulnerables de la red interna.

FW-108	Detección de conexiones desde múltiples fuentes fuera del cliente a un solo destino de la red interna	Identificar el exceso de intentos de conexión a una única dirección IP destino de la red interna desde al menos 100 direcciones IP externas en 5 minutos.
FW-110	Detección de conexiones internas hacia IP incluidas en listas negras (1er filtro)	Identificar conexiones de IP internas a direcciones IP consideradas maliciosas
FW-111	Detección de solicitudes DNS que no se pueden resolver.	Identificar picos altos de respuestas DNS del tipo NXDOMAIN (Non-Existent Domain), que es un indicador de infección de malware.
FW-112	Detección de archivos con contenido malware	Identificar archivos que contienen malware, y determinar cuál fue la acción realizada por el firewall.
FW-113	Detección de ataques de fuerza bruta hacia el protocolo SMB en servidores Windows.	Identificar ataques de fuerza bruta realizados hacia servidores Windows con la intención de obtener información de credenciales de usuarios SMB, servicios ofrecidos y recursos compartidos.
FW-114	Detección de ataques de fuerza bruta hacia el protocolo SMB en servidores Linux.	Identificar ataques de fuerza bruta realizados hacia servidores Linux con la intención de obtener información de credenciales de usuarios SMB, servicios ofrecidos y recursos compartidos.
FW-115	Detección de escaneos no autorizados hacia la infraestructura de la institución	Identificar escaneos no autorizados hacia la infraestructura de la institución. Detección de al menos 5 intentos de una misma ip origen

FW-116	Detección de ataques de directorio transversal hacia aplicaciones web.	Identificar ataques de directorio transversal dirigidos a aplicaciones web en la infraestructura de la institución.

Fuente: (Royal ITC,2021)

Posterior a la definición de casos de uso, se configuraron los mismos en la interfaz de graylog accediendo a la opción: Alerts→Event Definitions→Create Event Definition, tal como se muestra en la siguiente figura.

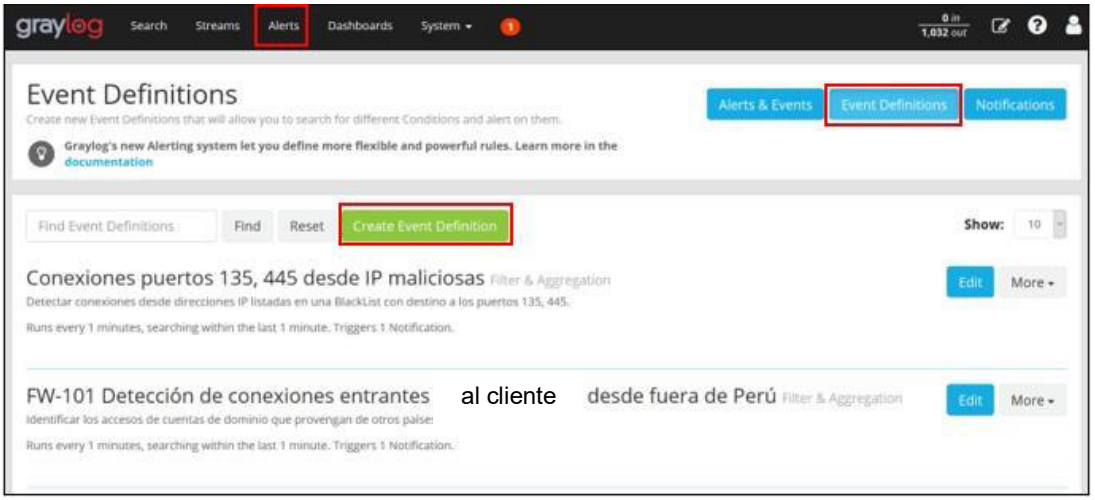

Figura 23 Pestaña Event Definitions

Fuente: (Royal ITC,2021)

Luego de acceder a la pestaña “Event Definitions”, se accede a la opción “Create Event Definitions” y se completaron los campos en la pestaña “Event Details” de acuerdo a los apartados:

Title → El título, nombre del caso de uso.
Description → Cuál es el objetivo del caso de uso.
Priority → Cuál es la prioridad: Alta, Media, Baja.
Luego se hace clic en “Next”

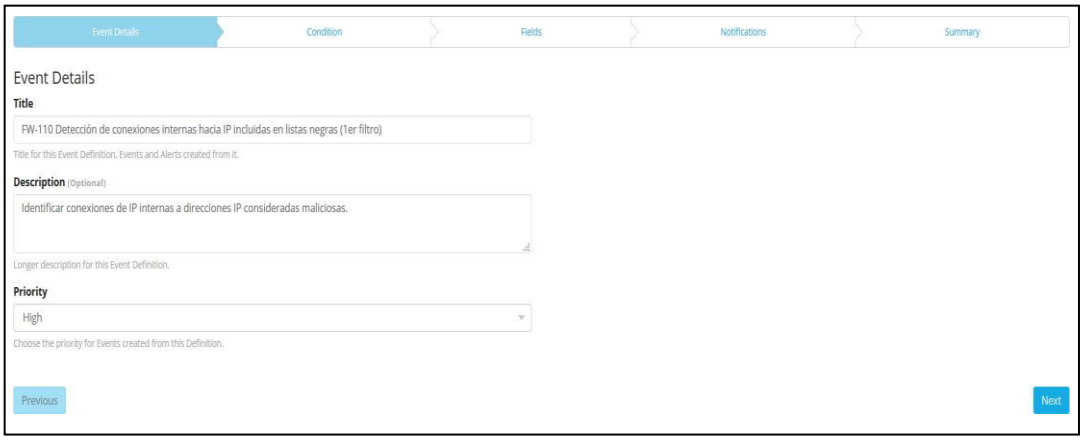

Figura 24 Pestaña Event Details
Fuente: (Royal ITC,2021)

Posterior a lo mencionado, se debe completar los campos en la pestaña "Conditions", de acuerdo a:

Condition Type → Seleccionar "Filter & Aggregation".
Search Query → Ingresar la consulta con los filtros que son relevantes para definir el evento.
Streams → Cuál es el flujo en donde se realizará la consulta. Dejarlo vacío en caso no se tenga configurado el stream para la tecnología.
Search within the last → Cuál es el intervalo de tiempo en el que se realizará la nueva búsqueda después de la última búsqueda.
Execute search every → Cada cuánto tiempo se ejecutará la búsqueda/consulta.

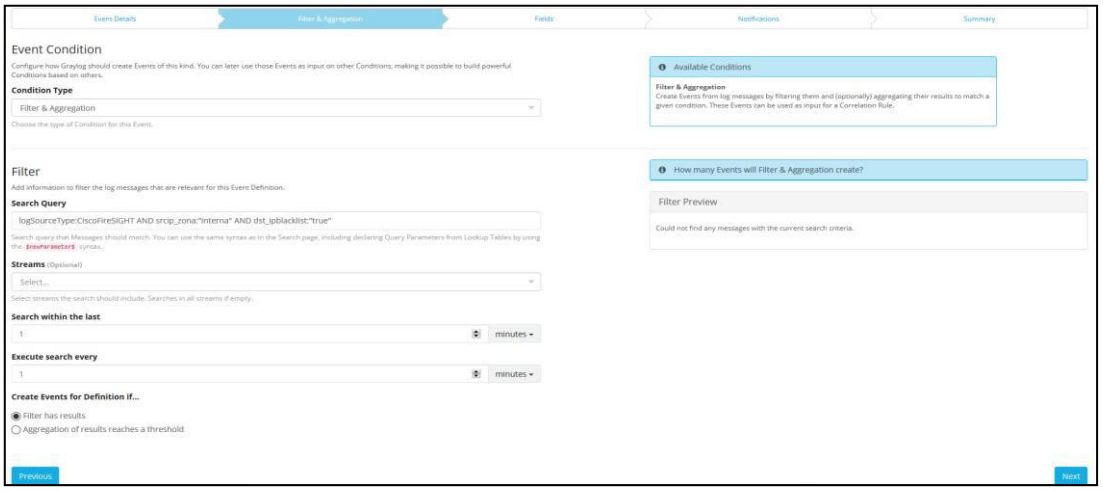

Figura 25 Pestaña Conditions
Fuente: (Royal ITC,2021)

Después de llenar los campos, hacer clic en “Next” y se debe completar los campos de la pestaña “Notifications” haciendo clic en “Add Notification”.

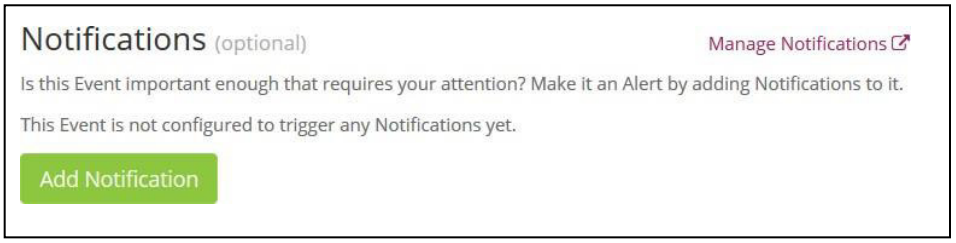

Figura 26 Pestaña Notifications

Fuente: (Royal ITC,2021)

En la pestaña “Add Notification” se debe escoger la notificación que fue creada previamente en la pestaña “Notofications”.

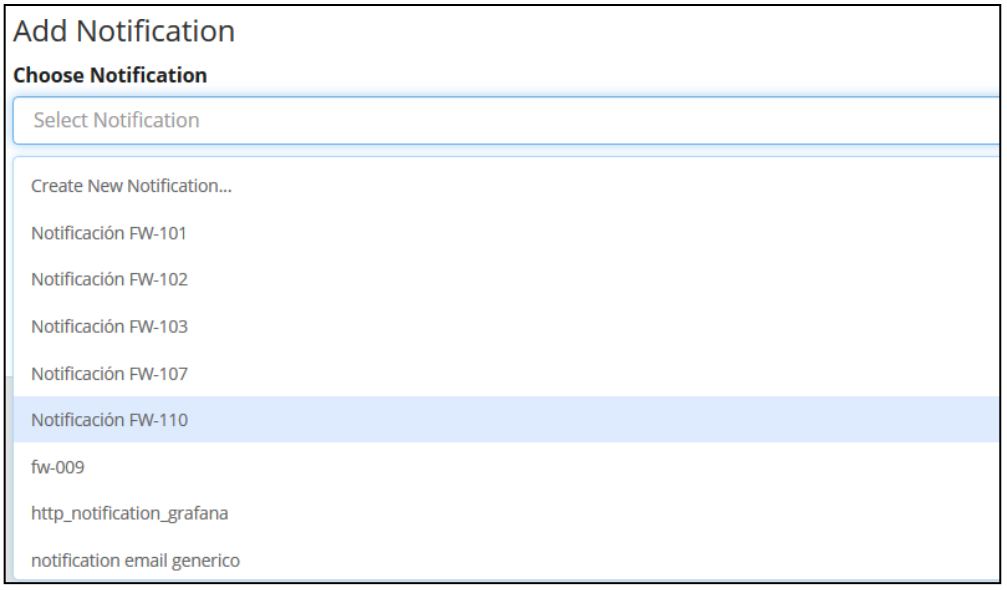

Figura 27 Pestaña Add Notifications

Fuente: (Royal ITC,2021)

Posterior a lo mencionado, se debe hacer clic en la opción “Done” que se muestra en la siguiente figura.

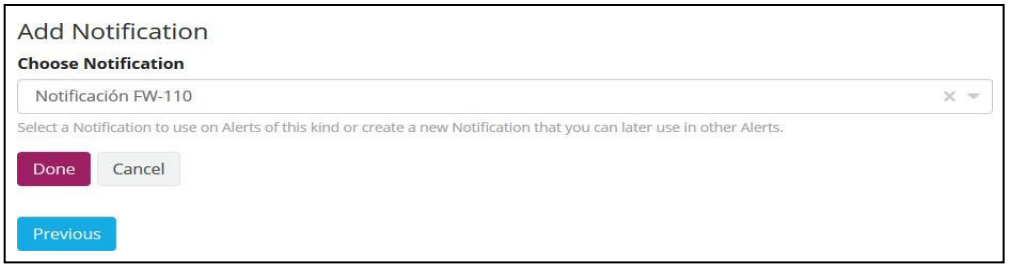

Figura 28 Opción Done

Fuente: (Royal ITC,2021)

Posterior a lo mencionado se habilitarán las siguientes configuraciones:

- Grace Period → En caso la cantidad de eventos que se generan en un caso de uso es un número considerable, se debe configurar un intervalo de tiempo para controlar cada cuánto tiempo el Graylog esperará para enviar notificaciones otra vez. Esto se hace con el fin de evitar sobrecargar el servidor de correo electrónico y los buzones configurados como receptores.
- Message Backlog → El número de mensajes que serán incluidos en las notificaciones. Como mínimo debe ir configurado el valor (1).

Finalmente se debe hacer clic en “Next”

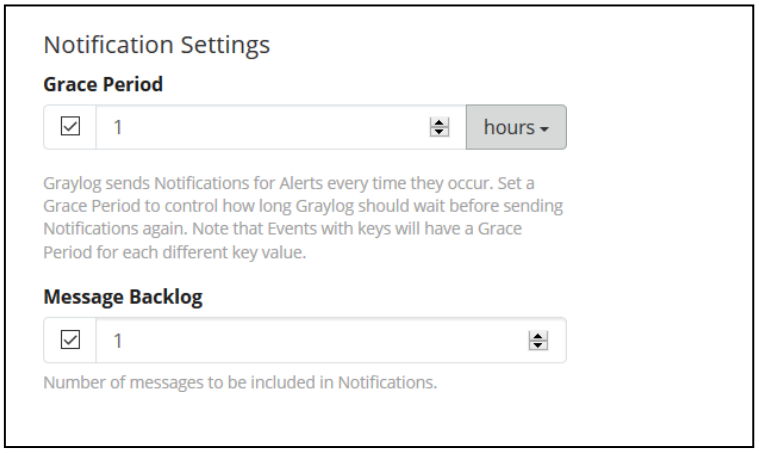

Figura 29 Ventana Notification Settings

Fuente: (Royal ITC,2021)

Posterior a hacer clic en “Next”, en la pestaña “Summary” se mostrará el resumen de la configuración que se ha realizado.

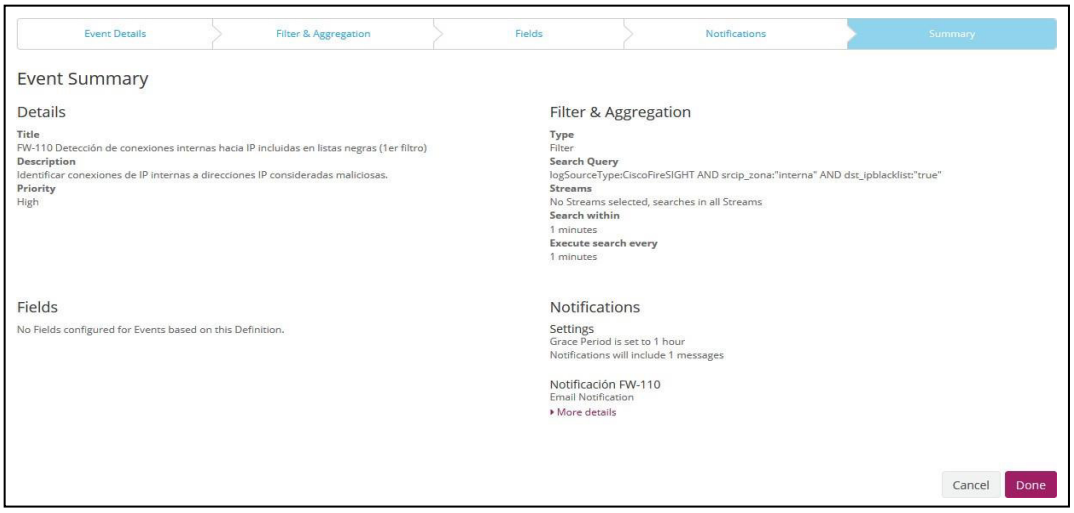

Figura 30 Pestaña Event Summary

Fuente: (Royal ITC,2021)

Hacer clic en “Done” y se observa que el evento se ha creado y aparece en la lista, tal como se muestra en la siguiente figura.

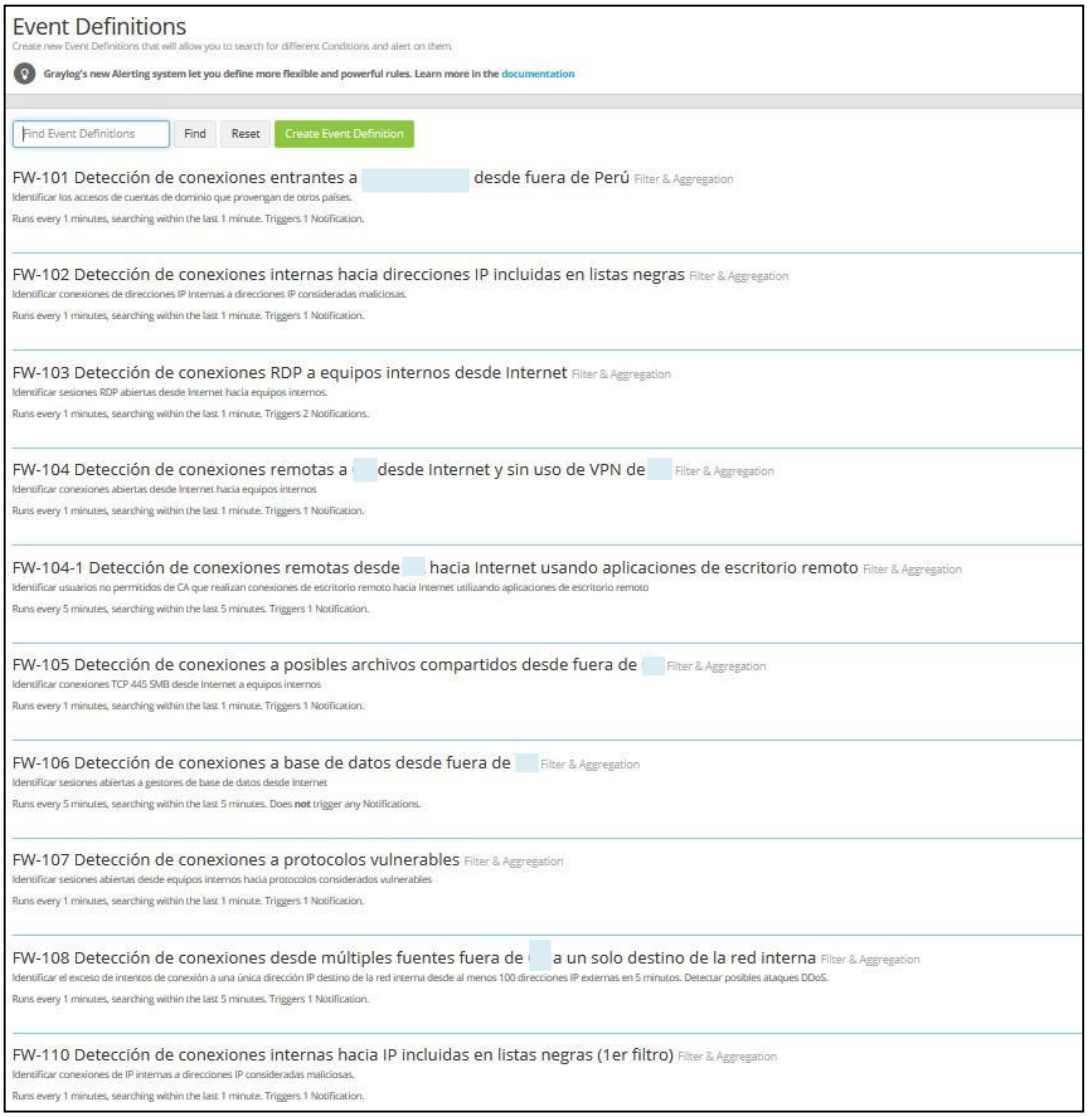

Figura 31 Pestaña Event Definitions con eventos creados

Fuente: (Royal ITC,2021)

El siguiente paso fue la configuración de notificaciones para los casos de uso, para lo cual se siguió la ruta: Alerts→ Notifications→ Create Notification; posterior a ello se completaron los campos:

Title → El título, nombre de la notificación para su identificación.
Description→ Una breve descripción de la notificación.
Notification Type → Seleccionar el tipo de la notificación. Para todos los casos de uso se está utilizando el tipo “Email Notification”.
Posterior a lo mencionado, se habilitaron más campos, los que se tuvieron que completar:
Sender → Cuál es la dirección de correo electrónico que debe ser usado como

remitente. Para todos los casos de uso se está usando la siguiente dirección de correo electrónico: yyy@royalcor.com

Subject → Cuál es el asunto que debe ser usado para la notificación por correo. Para todos los casos se está usando el título del evento definido. Dejar por defecto la siguiente configuración: Graylog event notification: {event_definition_title}

User recipient(s) → Cuál(es) usuario(s) de Graylog recibirán la notificación.

Email recipient(s) → Cuál(es) dirección(es) de correo electrónico recibirán la notificación.

Luego de completar los campos, se pasó a configurar la plantilla de cuerpo “Body Template” de la notificación que debía ser enviada por correo electrónico; el lenguaje usado fue el JMTE (Java Minimal Template Engine), tal como se muestra en la siguiente figura.

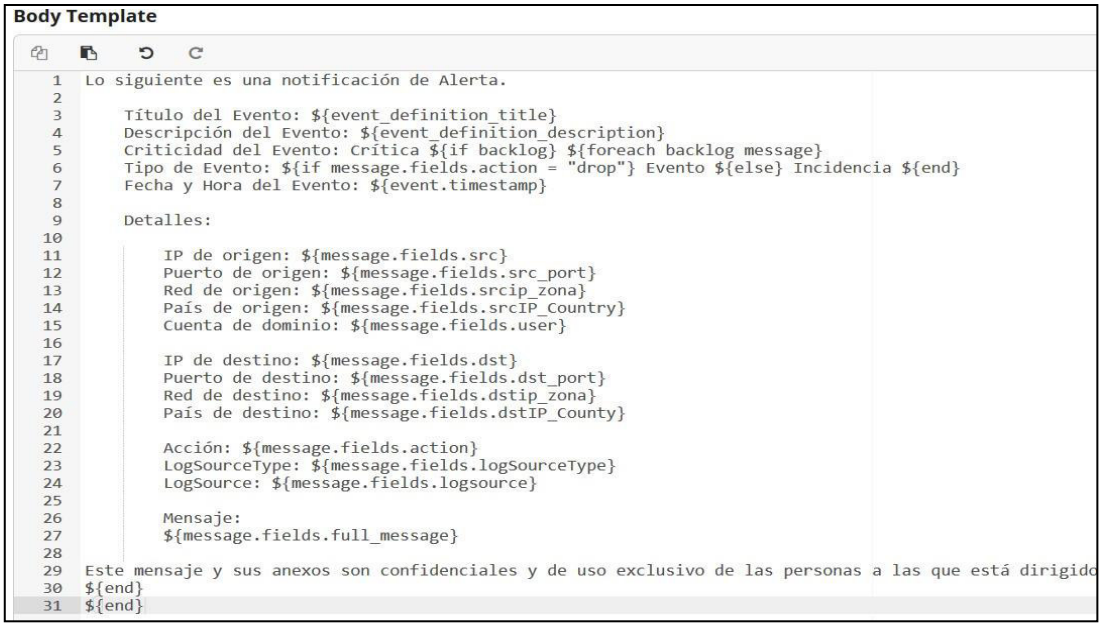

Figura 32 Configuración de plantilla de cuerpo “Body Template”

Fuente: (Royal ITC,2021)

Posterior a todo lo mencionado, se ejecutó una notificación de prueba que debía llegar a través de un correo al buzón configurado, para ello se hizo clic en la opción “Create”.

Figura 33 Pestaña Test Notification

Fuente: (Royal ITC,2021)

Finalmente se debía verificar que la notificación se había creado y si aparecía en la lista de notificaciones.

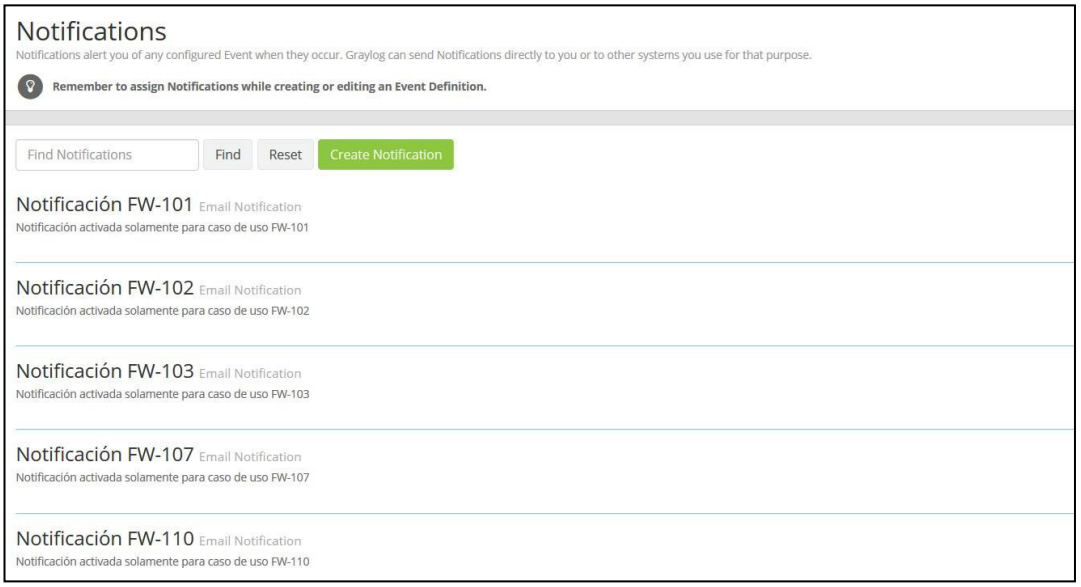

Figura 34 Validación de Notificación

Fuente: (Royal ITC,2021)

Procedimiento de gestión de análisis forense

Se establecieron procedimientos para la aplicación del análisis forense, la

detección y recuperación de evidencias en dispositivos de almacenamiento, teniendo como fin mantener la integridad de la información, se muestran dichos procedimientos en las tablas mostradas en el ANEXO 03 y en las siguientes ilustraciones.

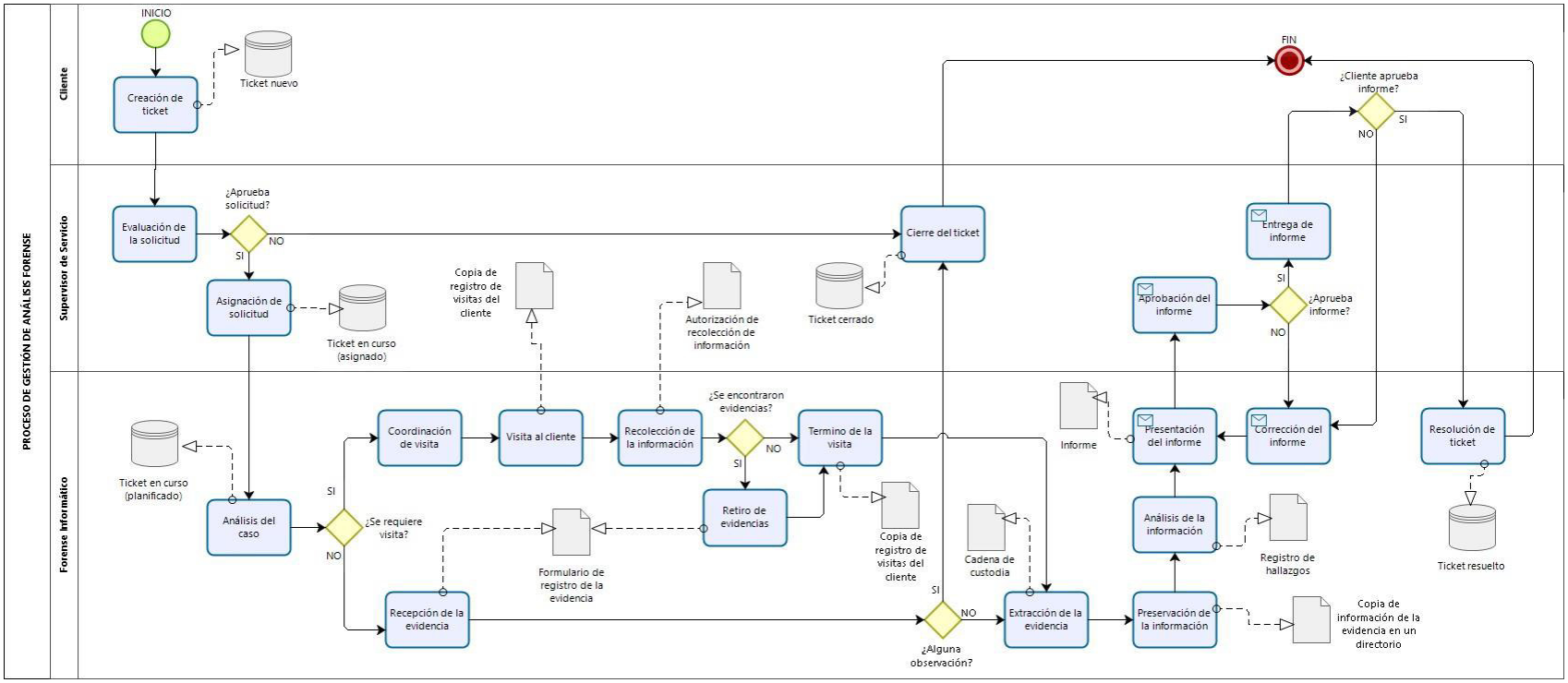

Figura 35 Diagrama de procedimiento de aplicación de análisis forense

Fuente: (Royal ITC,2021)

Anexo 09: Eventos e incidentes alertados por PRTG

Semana	Down	Warning	Unusual	Paused	Total
01/05/2021- 02/05/2021	233	2	58	2	295
03/05/2021- 09/05/2021	590	21	260	44	915
10/05/2021- 16/05/2021	505	14	211	7	737
17/05/2021- 23/05/2021	466	15	223	15	719
24/05/2021- 30/05/2021	438	11	262	43	754
31/05/2021	60	2	27	2	91
Total	2292	65	1041	113	3511

Anexo 10: Cumplimiento de tiempos de solución de incidentes

Fecha de solución	A Tiempo	Vencido	No solucionado	Total
01/05/2021-02/05/2021	64	41	0	105
03/05/2021-09/05/2021	224	76	0	300
10/05/2021-16/05/2021	163	97	0	260
17/05/2021-23/05/2021	72	169	0	241
24/05/2021-30/05/2021	107	91	1	199
31/05/2021	30	0	0	30
Total	660	474	1	1135

Anexo 11: Detalle de incidentes de seguridad por nivel de criticidad

Incidentes de seguridad por nivel de criticidad - mayo 2021						
	Semana	**Crítico**	**Alto**	**Medio**	**Bajo**	**Total**
Mayo-2021	Semana 1 01/05/2021- 02/05/2021	1	11	0	0	12
	Semana 2 03/05/2021- 09/05/2021	2	344	0	0	346
	Semana 3 10/05/2021- 16/05/2021	0	183	0	0	183
	Semana 4 17/05/2021- 23/05/2021	0	137	0	0	137
	Semana 5 24/05/2021- 30/05/2021	0	163	0	0	163
	Semana 6 31/05/2021	0	24	0	0	24
	Total	3	862	0	0	865

Anexo 12: Detalle de eventos e incidentes de seguridad por caso de uso

Caso de uso	N° de eventos detectados	N° de incidentes reportados
FW-101 Detección de conexiones entrantes al cliente desde fuera del Perú	0	3
FW-102 Detección de conexiones internas hacia direcciones IP incluidas en listas negras	0	0
FW-103 Detección de conexiones RDP a equipos internos desde internet	0	0
FW-104 Detección de conexiones remotas hacia el cliente desde internet y sin uso del VPN del cliente	0	856
FW-105 Detección de conexiones a posibles archivos compartidos desde fuera del cliente	0	6
FW-107 Detección de conexiones a protocolos vulnerables	0	0
FW-108 Detección de conexiones desde múltiples fuentes fuera del cliente a un solo destino de la red interna	0	0
FW-110 Detección de conexiones internas hacia IP incluidas en listas negras	0	0
FW-111 Detección de solicitudes DNS que no se pueden resolver	0	0
FW-112 Detección de archivos con contenido malware	0	0
Total	0	865

Anexo 13: Resultados

Resultados sobre monitoreo de plataforma

Se realizó el monitoreo de plataforma, en el cual se registraron la alerta según incidente o evento, basándose en cinco estados de PRTG: DOWN, WARNING, UNUSUAL, PAUSED, UNKNOWN, esta información se registre como ticket o como bitácora según sea la clasificación, en la figura siguiente se muestra el registro de alertas según el tipo de registro y la clasificación.

REGISTRO DE ALERTAS					
REGISTRO	DOWN	WARNING	UNUSUAL	PAUSED	UNKNOWN
TICKET	SI	SI	NO	NO	SI
BITÁCORA	SI	SI	SI	SI	SI

Figura 36 Registro de eventos e incidentes

Fuente: (Royal ITC,2021)

Dentro del proceso de monitoreo de plataformas se da reinicio a los equipos bantotal, que son un conjunto de 56 equipos distribuidos en 8 grupos, este reinicio no puede ser mayor a 30 minutos, ya que si no debe ser reportado como incidencia. El reinicio se realiza de turno noche entre las 8:00 pm a 8:00 am. En la siguiente figura se muestra la clasificación de los reinicios de equipos bantotal.

EQUIPOS BANTOTAL - REINICIO 08:00 pm - 08:00 am			
	DOWN	Menor e igual a 30 minutos	Mayor a 30 minutos
Alerta	Evento	SI	NO
	Incidente	NO	SI
Registro	TICKET	NO	SI
	BITÁCORA	SI	SI

Figura 37 Reinicio equipos bantotal

Fuente: (Royal ITC,2021)

Los registros en estado UNKNOWN fueron coordinados para que se reporten 30 minutos de haber iniciado el incidente, considerando la criticidad del activo. En la figura siguiente se muestra el registro del nuevo estado de

monitoreo.

ESTADO UNKNOWN			
	UNKNOWN ?	Menor e igual a 30 minutos	Mayor a 30 minutos
Alerta	Evento	SI	NO
	Incidente	NO	SI
Registro	TICKET	NO	SI
	BITÁCORA	SI	SI

Figura 38 Registro de nuevo estado de monitoreo

Fuente: (Royal ITC,2021)

Todos estos registros que muestra la herramienta PRGT son compilados en la bitácora de monitoreo, La siguiente figura muestra el registro de eventos e incidentes de monitoreo de plataformas donde se muestran los campos de la bitácora: ITEM, Fecha De Alerta, Hora De Alerta, Fecha De Notificación, Hora De Notificación, Tiempo De Notificación, Fecha De Fin, Hora Fin, Tiempo Solución, Tipo De Alerta, Categoría, Plataforma, Servidor, Ubicación Del Problema – Sensor, Nivel De Criticidad, Turno, Monitor Responsable, Ticket (Sistema Integrado) Royal ITC. Causa De Alerta, Responsable, SLA Incidente, Cumplimiento SLA Incidente, SLA Evento, Cumplimiento SLA Evento y Ruta.

JULIO

17/07/2021

ROYAL ITC

REPORTE DIARIO DE MONITOREO

	FECHA DE ALERTA	HORA DE ALERTA	FECHA DE NOTIFICACIÓN	HORA DE NOTIFICACIÓN	TIEMPO DE NOTIFICACIÓN	FECHA DE FIN	HORA FIN	TIEMPO SOLUCIÓN	TIPO DE ALERTA	CATEGORIA	PLATAFORMA	SERVIDOR
1	13/07/2020	15:58	13/07/2020	16:01	00:03:00				WARNING	SERVIDOR	MONITOREO TI	wde1051
2	24/08/2020	10:44	24/08/2020	10:44	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	076
3	30/11/2020	17:25	30/11/2020	17:25	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	cido
4	01/10/2020	13:59	01/10/2020	13:59	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	ıales
5	08/02/2021	19:44	08/02/2021	19:44	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	cido
6	17/02/2021	16:02	17/02/2021	16:13	00:11:00				WARNING	SERVIDOR	MONITOREO TI	cido
7	05/03/2021	18:55	05/03/2021	18:55	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	cido
8	14/03/2021	04:02	14/03/2021	04:08	00:06:50				WARNING	SERVIDOR	MONITOREO TI	35
9	17/03/2021	12:42	17/03/2021	12:42	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	36
10	17/03/2021	12:42	17/03/2021	12:42	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	36
11	17/03/2021	12:42	17/03/2021	12:42	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	36
12	17/03/2021	12:42	17/03/2021	12:42	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	36
13	05/04/2021	09:26	05/04/2021	09:33	00:06:06				WARNING	SERVIDOR	MONITOREO TI	73
14	07/05/2021	09:47	07/05/2021	09:47	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	BD
15	09/05/2021	21:33	09/05/2021	21:33	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	VEB
16	09/05/2021	21:32	09/05/2021	21:32	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	BI
17	19/05/2021	10:40	19/05/2021	10:45	00:04:39				WARNING	SERVIDOR	MONITOREO TI	1051
18	20/05/2021	08:36	20/05/2021	08:36	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	cido
19	20/05/2021	08:36	20/05/2021	08:36	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	cido
20	20/05/2021	08:36	20/05/2021	08:36	00:00:00				PAUSADO	SERVIDOR	MONITOREO TI	cido
21	31/05/2021	12:30	31/05/2021	12:47	00:17:26				PAUSADO	SERVIDOR	MONITOREO TI	12
22	03/06/2021	19:57	03/06/2021	20:01	00:04:42				WARNING	SERVIDOR	MONITOREO TI	cido
23	07/06/2021	06:03	07/06/2021	06:16	00:13:29				WARNING	SERVIDOR	MONITOREO TI	Canales
24	07/06/2021	08:10	07/06/2021	08:15	00:05:23	17/07/2021	01:10	952:55:00	WARNING	SERVIDOR	MONITOREO TI	0.0.201.113)
25	10/06/2021	01:13	10/06/2021	01:24	00:11:01				WARNING	SERVIDOR	MONITOREO TI	cido
26	11/06/2021	06:40	11/06/2021	06:53	00:13:36				WARNING	SERVIDOR	MONITOREO TI	cido
27	13/06/2021	03:21	13/06/2021	03:30	00:09:12				WARNING	SERVIDOR	MONITOREO TI	rido
28	15/06/2021	06:12	15/06/2021	06:12	00:00:00				CAÍDA	SERVIDOR	MONITOREO TI	055
29	21/06/2021	17:51	21/06/2021	17:55	00:04:10				WARNING	SERVIDOR	MONITOREO TI	cido
30	22/06/2021	00:01	22/06/2021	00:01	00:00:00				INUSUAL	SERVIDOR	MONITOREO TI	01
31	23/06/2021	13:50	23/06/2021	14:01	00:11:28				WARNING	SERVIDOR	MONITOREO TI	cido

Figura 39 Modelo de reporte diario de monitoreo

Fuente: (Royal ITC,202

Los eventos e incidentes que se registraron durante el mes de mayo del 2021 se detallan en la tabla del Anexo 04; estos fueron registrados a diario e hicieron un total de 1135 incidentes y 2337 eventos, tal como se muestra en la siguiente figura.

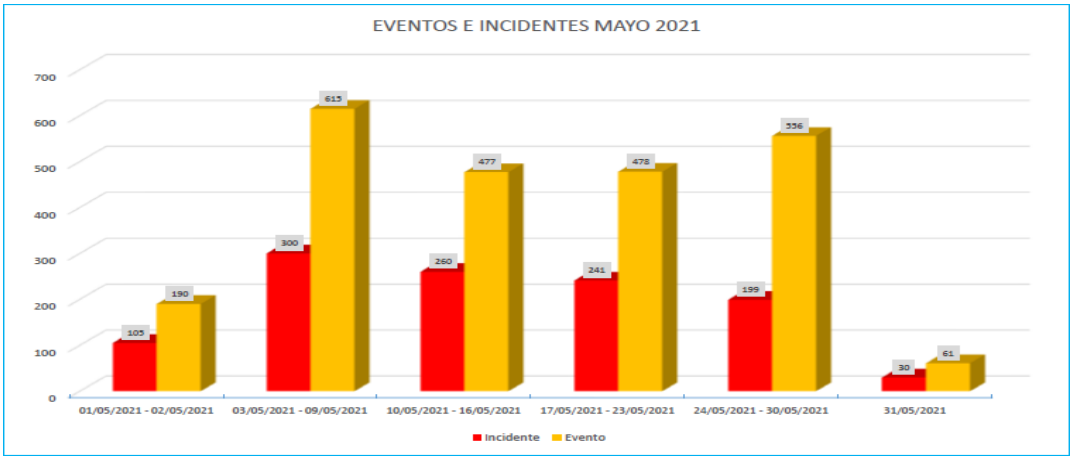

Figura 40 Eventos e incidentes mes de mayo

Fuente: (Royal ITC,2021)

De acuerdo a la Figura presentada anteriormente, se puede observar que la mayoría de los eventos reportados se resolvieron en el mismo día que fueron alertados. Respecto al nivel de criticidad de incidentes reportados, la mayoría de los incidentes fueron categorizados con niveles críticos, tal como se muestra en la tabla del Anexo 06 y en la siguiente figura.

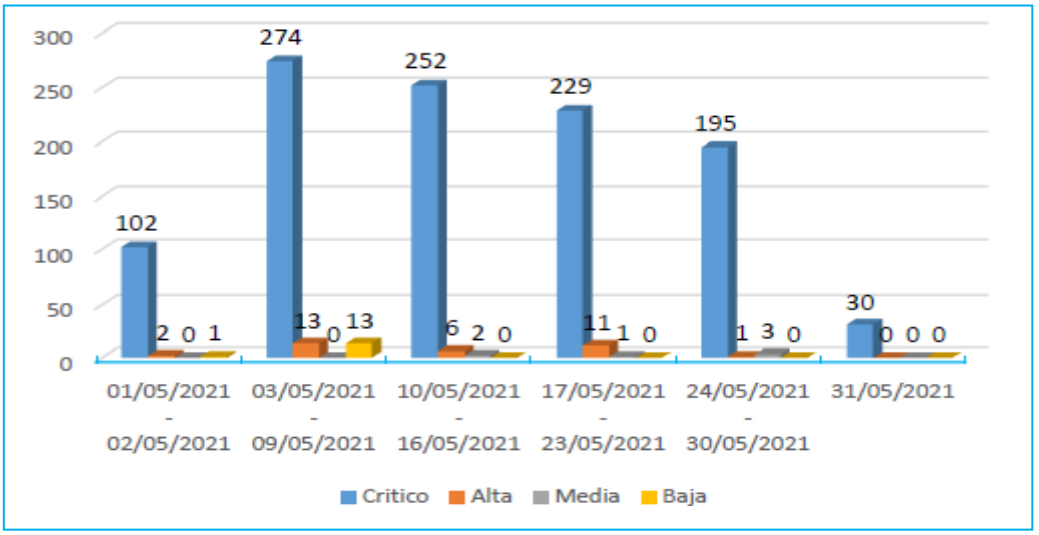

Figura 41 Incidentes por nivel de criticidad en el mes de mayo

Fuente: (Royal ITC,2021)

Respecto al nivel de criticidad de eventos reportados, la mayoría de los eventos fueron categorizados con niveles críticos, tal como se muestra en la tabla del Anexo 07 y en la siguiente figura.

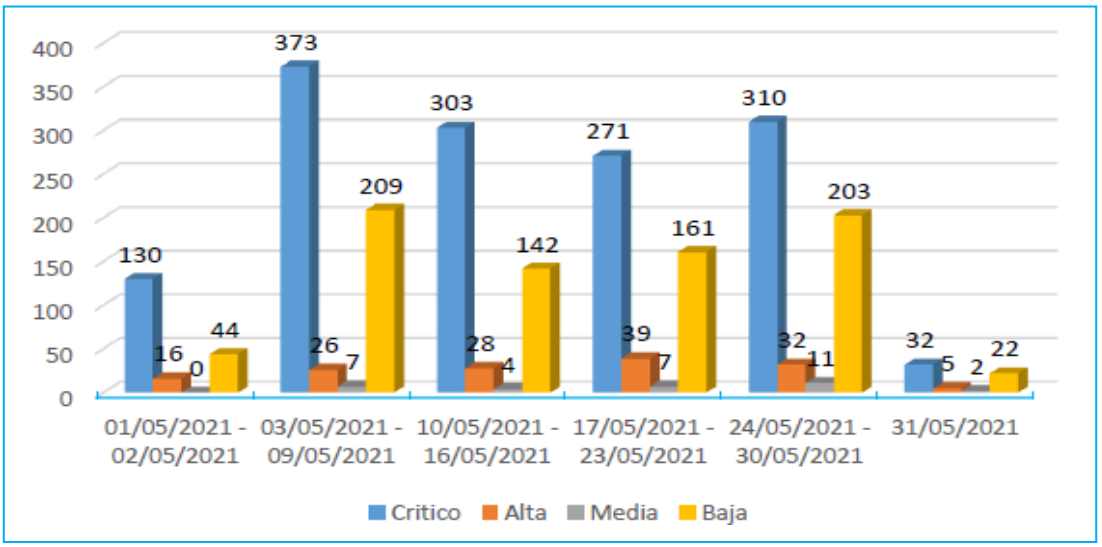

Figura 42 eventos por nivel de criticidad en el mes de mayo

Fuente: (Royal ITC,2021)

Respecto al funcionamiento de la herramienta PRTG, esta hizo reportes de estados de plataformas de acuerdo con la clasificación que se presenta en la siguiente tabla.

Tabla 8 Estado de PRTG

ESTADO	DESCRIPCIÓN
Down	PRTG no puede alcanzar el dispositivo o el sensor ha detectado un error.
Warning	El sensor detectó un error y muestra un estado de Advertencia , pero PRTG está intentando comunicarse nuevamente con el dispositivo monitoreado. El sensor puede cambiar de pronto a un estado inactivo.
Unusual	El sensor informa valores inusuales para ese día de la semana y la hora del día. La detección inusual se basa en los datos promedio históricos del sensor.

Paused	El sensor está en pausa durante un periodo de tiempo determinado, indefinidamente o debido a una dependencia.
Unknown	El sensor aún no ha recibido ningún dato o hay un error en la comunicación (de red), probablemente en el sistema de la sonda.

Fuente: (Royal ITC,2021)

En la tabla del Anexo 09 se describen los eventos e incidentes alertados por la herramienta PRTG a partir del 01 de mayo hasta el 31 de mayo del 2021, tal como se muestra en la siguiente figura.

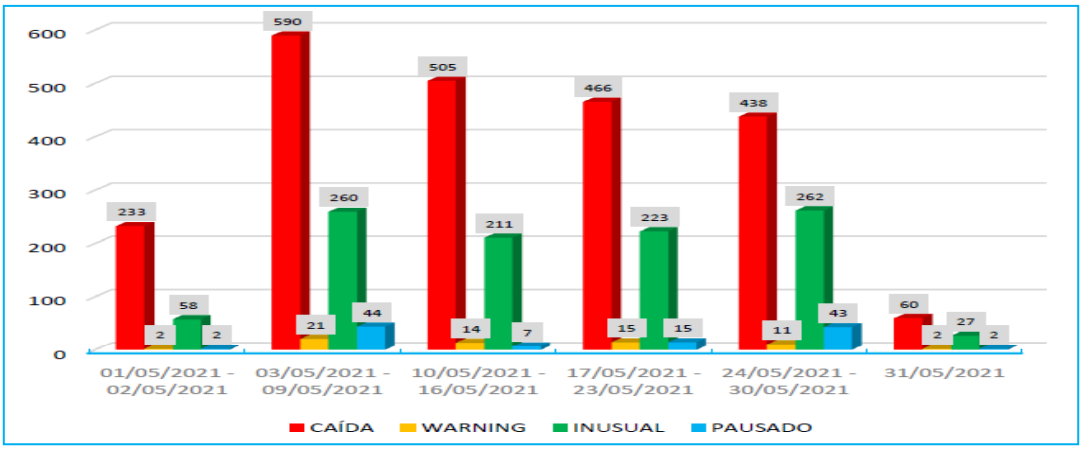

Figura 43 Alertas de PRTG

Fuente: (Royal ITC,2021)

De acuerdo a la figura anterior, se puede observar que la mayoría de eventos e incidentes alertados por la herramienta PRTG fueron de caídas en las diferentes plataformas, también se observa alertas considerables de eventos e incidentes inusuales, los mismos que debieron ser solucionados en un determinado tiempo; respecto al tiempo de solución de los incidentes el cliente estableció que los mismos debían ser resueltos de acuerdo a su nivel de complejidad y criticidad, tal como se muestra en las siguientes tablas.

Tabla 9 Niveles de solución de incidentes

Nivel de complejidad de resolución del incidente	
Nivel	**Descripción**
A	Se requiere solo personal propio del cliente
B	Se requiere participación del personal del proveedor
C	Se requiere participación de la marca de producto

Fuente: (Royal ITC,2021)

Tabla 10 Tiempos de resolución de incidentes

Tiempo de resolución de incidentes			
Nivel de criticidad	**Nivel de complejidad**		
	A	**B**	**C**
Bajo	48 horas	72 horas	14 días
Medio	24 horas	48 horas	7 días
Alto	12 horas	36 horas	5 días
Crítico	4 horas	24 horas	2 días

Fuente: (Royal ITC,2021)

De acuerdo con el registro en bitácora, se obtuvieron resultados acerca del cumplimiento de los tiempos de solución de incidentes durante el mes de mayo que se detallan en la tabla del Anexo 10 y en la siguiente figura.

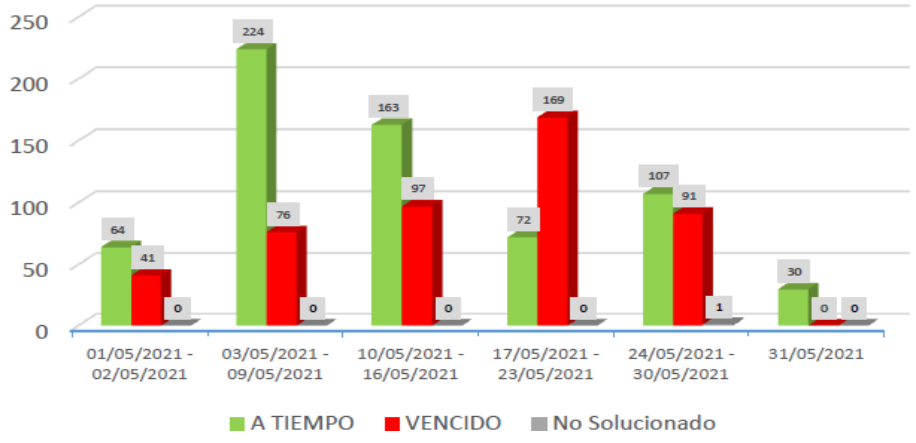

Figura 44 Cumplimiento de tiempos de solución de incidentes

Fuente: (Royal ITC,2021)

Los eventos e incidentes registrados durante el mes de mayo se definieron de acuerdo con el nivel de criticidad de los equipos tecnológicos que formaron parte del alcance del servicio, tal como se muestra en la siguiente tabla.

Tabla 11 Niveles de criticidad para eventos e incidencias de seguridad

Criticidad del activo tecnológico	Nivel de criticidad para eventos e incidencias
1	Crítica
2	Alta
3	Media
4	Baja

Fuente: (Royal ITC,2021)

La cantidad de incidentes de seguridad registrados por nivel de criticidad, desde el 01 de mayo al 31 de mayo del 2021 se detalla en la tabla del Anexo 11 y en la siguiente figura.

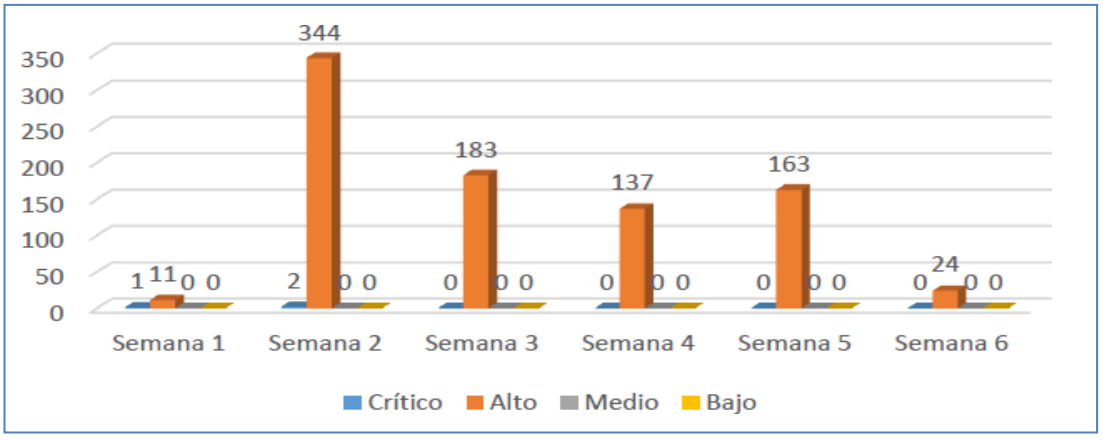

Figura 45 Registro de incidentes de seguridad por nivel de criticidad

Fuente: (Royal ITC,2021)

De acuerdo con la figura anterior, se puede observar que la mayoría de los incidentes de seguridad registrados se clasificaron por tener niveles altos respecto a su criticidad; en cuanto a los eventos e incidentes registrados por casos de uso, se observa en la tabla del Anexo 12 y en la siguiente figura el detalle de eventos e incidentes de seguridad registrados por caso de uso desde el 01 de mayo al 31 de mayo del 2021

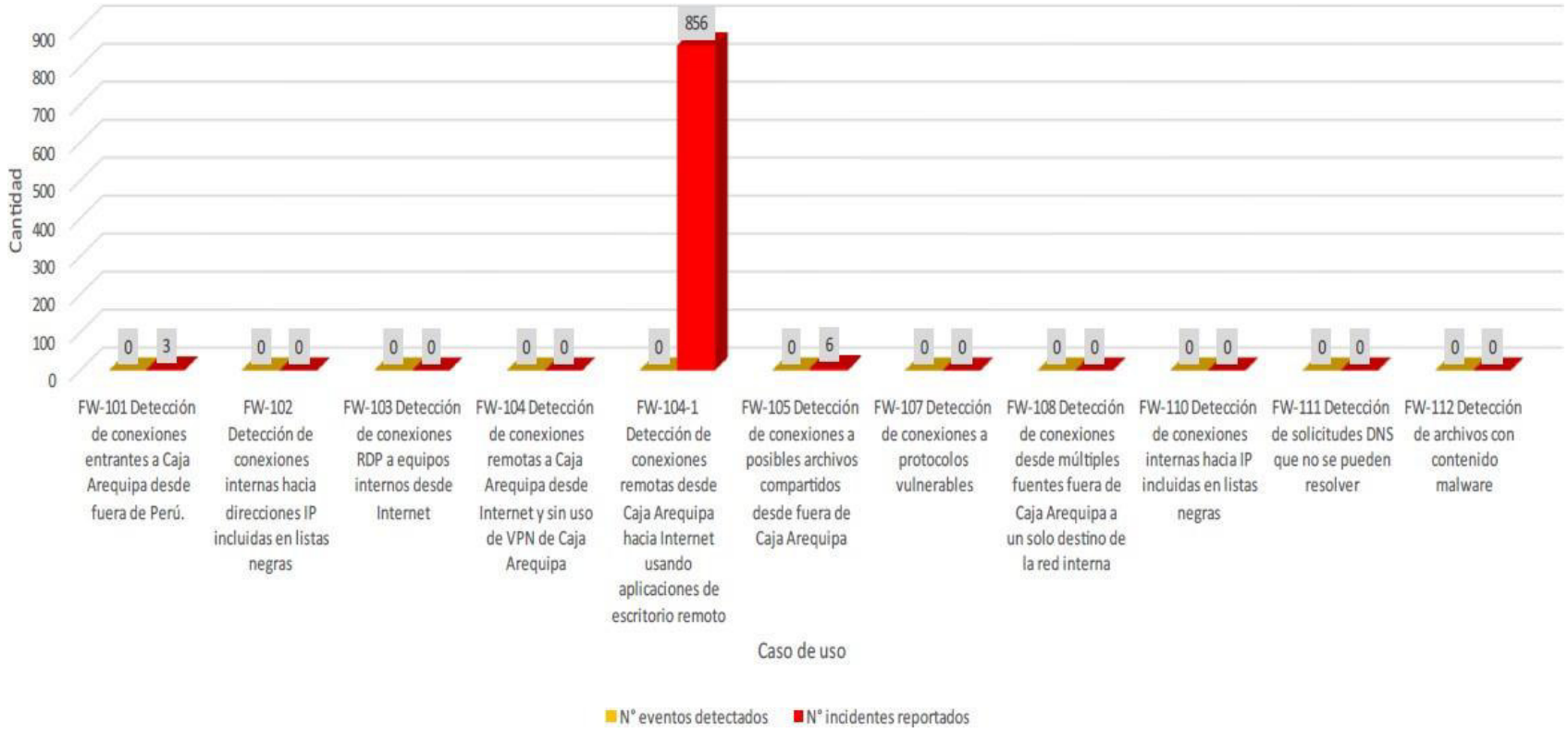

Figura 46 Registro de eventos e incidentes de seguridad por caso de uso

Fuente: (Royal ITC,2021)

De acuerdo al registro de eventos e incidentes de seguridad por caso de uso mostrado en la figura anterior, se observa que la mayoría fueron incidentes de seguridad respecto a las conexiones remotas desde el cliente hacia internet usando aplicaciones de escritorio remoto.

Respecto al cumplimiento de SLA de eventos e incidentes de TI, la siguiente tabla muestra el cumplimiento de SLA de incidentes desde el 01 de mayo al 31 de mayo del 2021.

Tabla 12 Cumplimiento de SLA de incidentes de TI

Cumplimiento de SLA- Incidentes de TI	**Alertas**
Si cumple	1135
No cumple	0
Total	1135

Fuente: (Royal ITC,2021)

De acuerdo a la tabla anterior se puede observar que se cumplieron con todos los SLA de incidentes de TI; respecto a los eventos de TI, la siguiente tabla muestra el cumplimiento de SLA de eventos de TI desde el 01 de mayo hasta el 31 de mayo.

Tabla 13 Cumplimiento de SLA de eventos de TI

Cumplimiento de SLA- Eventos de TI	**Alertas**
Si cumple	2377
No cumple	0
Total	2377

Fuente: (Royal ITC,2021)

De acuerdo con la tabla anterior se puede observar que se cumplieron con todos los SLA de eventos de TI; respecto al cumplimiento de SLA de eventos de seguridad desde el 01 de mayo al 31 de mayo del 2021, no se presentaron durante el mes eventos de seguridad, sin embargo, el cumplimiento de SLA de incidentes de seguridad si se cumplieron en su

totalidad durante el mes, tal como se muestra en la siguiente tabla.

Tabla 14 Cumplimiento de SLA de incidentes de seguridad

Cumplimiento de SLA- Eventos de TI	Alertas
Si cumple	865
No cumple	0
Total	865

Fuente: (Royal ITC,2021)

Resultados sobre la gestión de vulnerabilidades

La gestión de vulnerabilidades fue desarrollada en un Dashboard, para el mes de mayo se obtuvo un total de 320 vulnerabilidades en la fase 1, de los cuales 10 fueron críticas, 5 altas, 21 media, 1 baja y 283 informativas. En la siguiente figura se muestra la distribución de la cantidad de vulnerabilidades para el mes de mayo.

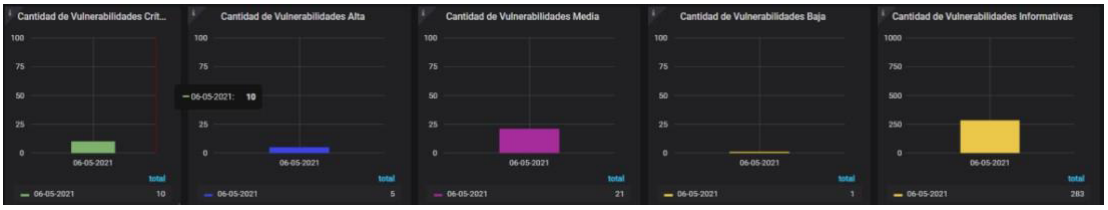

Figura 47 Registro de vulnerabilidades según tipo para el mes de mayo

Fuente: (Royal ITC,2021)

En cuanto al mes de junio, se desarrolló el análisis de vulnerabilidades en 55 servidores, de donde se obtuvo un total de 549 vulnerabilidades en fase 1, de los cuales 9 fueron críticas, 22 altas, 56 media, 1 baja y 461 informativas. En la siguiente figura se muestra la distribución de la cantidad de vulnerabilidades para el mes de mayo.

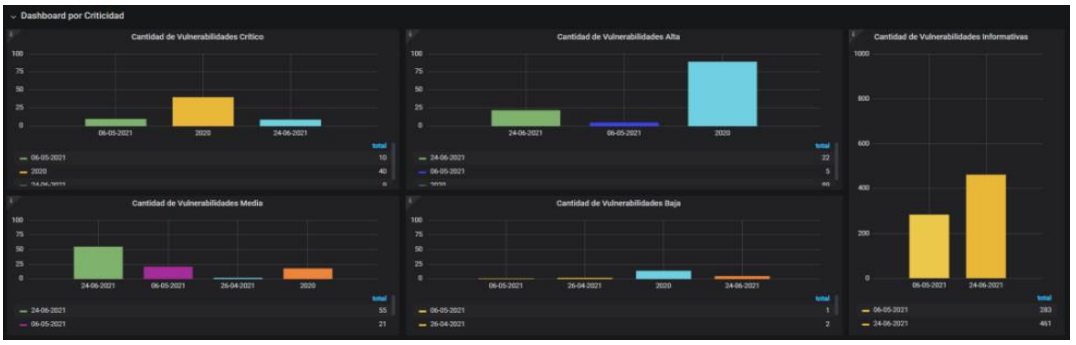

Figura 48 Registro de vulnerabilidades según tipo para el mes de junio

Fuente: (Royal ITC,2021)

Resultados de respuesta ante incidentes

En la Figura siguiente se muestra los tiempos de respuesta según el nivel de criticidad y nivel de complejidad. Estos fueron dependientes del incidente, por lo que se pudo apreciar que existieron varios trabajos que sobrepasaron el tiempo de resolución.

Tiempos de resolución de incidentes			
	Nivel de Complejidad		
Nivel de Criticidad	A	B	C
Bajo	48 horas	72 horas	14 días
Medio	24 horas	48 horas	7 días
Alto	12 horas	36 horas	5 días
Critico	4 horas	24 horas	2 días

Figura 49 Tiempo de resolución de incidentes

Fuente: (Royal ITC,2021)

En la siguiente Figura se muestra un listado del cumplimiento del tiempo de solución, donde se evidencia que de un total de 1135 incidentes, 660 (58.15%) incidentes si fueron solucionados a tiempo, 474 incidentes fueron solucionados por fuera del tiempo de resolución y solamente 1 incidente no fue solucionado.

Fecha de Solución	A TIEMPO	VENCIDO	No Solucionado	Total
01/05/2021 - 02/05/2021	64	41	0	105
03/05/2021 - 09/05/2021	224	76	0	300
10/05/2021 - 16/05/2021	163	97	0	260
17/05/2021 - 23/05/2021	72	169	0	241
24/05/2021 - 30/05/2021	107	91	1	199
31/05/2021	30	0	0	30
Total	**660**	**474**	**1**	**1135**

Figura 50 Cumplimiento tiempo de resolución de incidentes

Fuente: (Royal ITC,2021)

En la Figura siguiente se puede apreciar el tiempo máximo de solución ante incidentes con solución interna, teniendo en cuenta solo un día de tiempo de solución, se puede apreciar que el día 17 de julio se logró solucionar 38 incidentes y 3 incidentes no fueron solucionados.

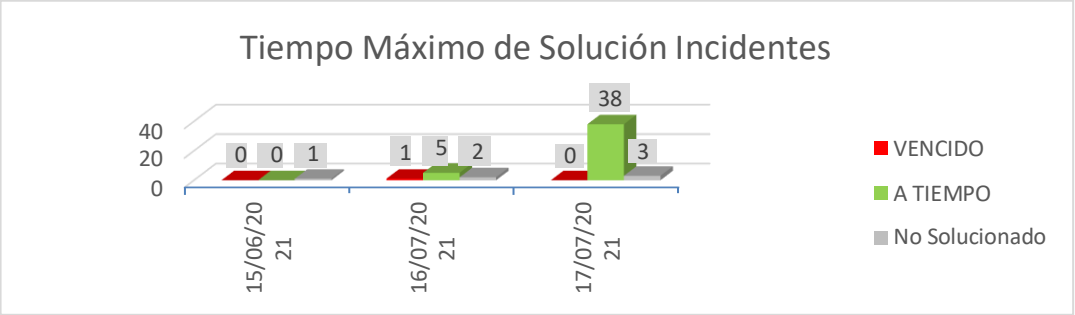

Figura 51 Tiempo máximo de solución de incidentes

Fuente: (Royal ITC,2021)

En la Figura anterior se puede observar mayor número de eventos registrados que incidentes durante el mes de mayo, pero también el número de incidentes por semana fue considerable por lo que se requirieron acciones para resolver dichos incidentes y eventos, se muestra el detalle del número de incidentes y eventos resueltos en la tabla del Anexo 05 y en la siguiente figura.

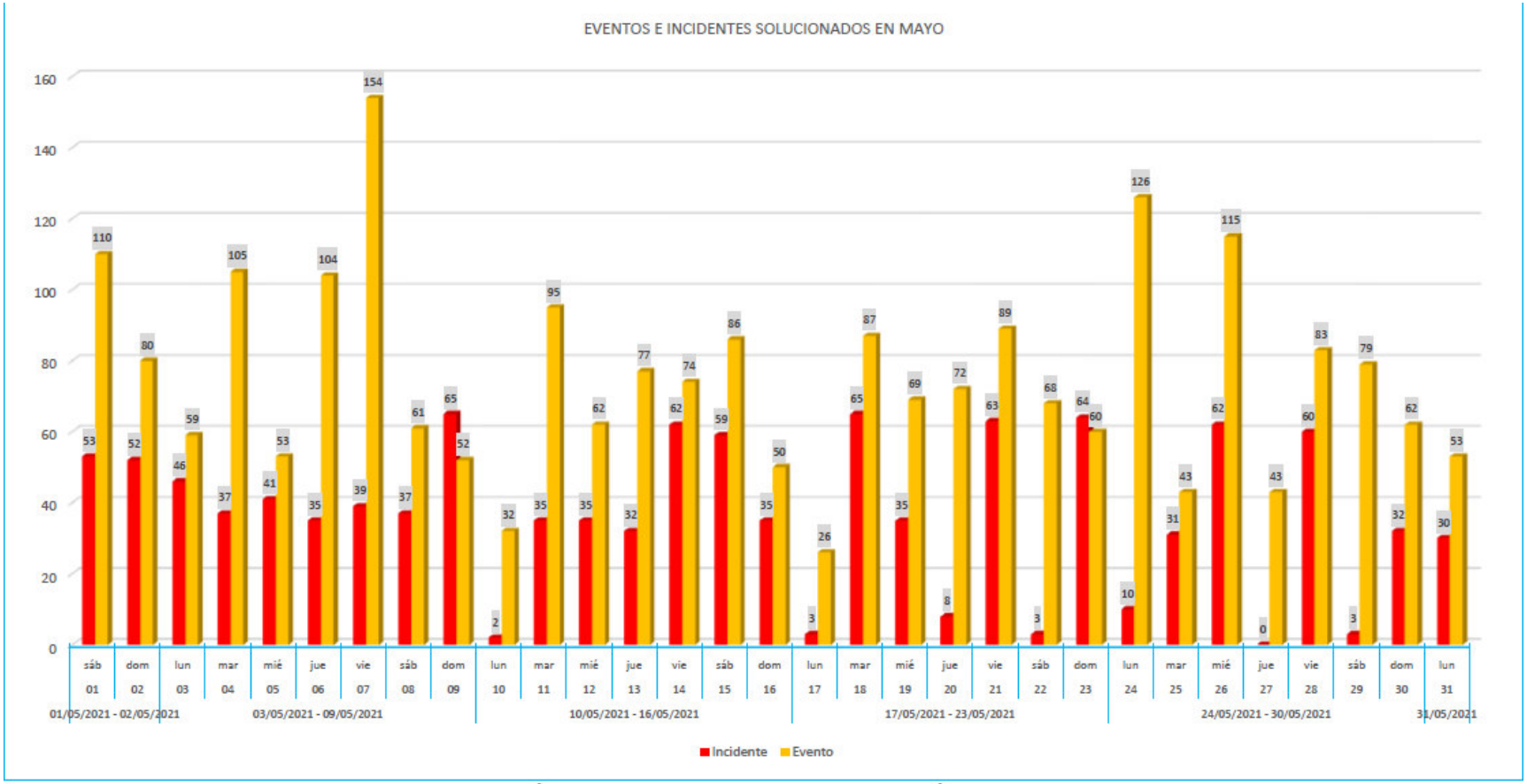

Figura 52 Eventos e incidentes resueltos mes de mayo

Fuente: (Royal ITC,2021)

De acuerdo con la Figura anterior mostrada, se puede observar un gran número de eventos e incidentes resueltos por día, casi la totalidad de estos de acuerdo a la tabla mostrada en el Anexo 05; sin embargo, no todos los incidentes y eventos que se reportaban se resolvieron al instante o en el mismo día, se presenta en la siguiente figura el comportamiento de incidentes alertados y resueltos en el mismo día.

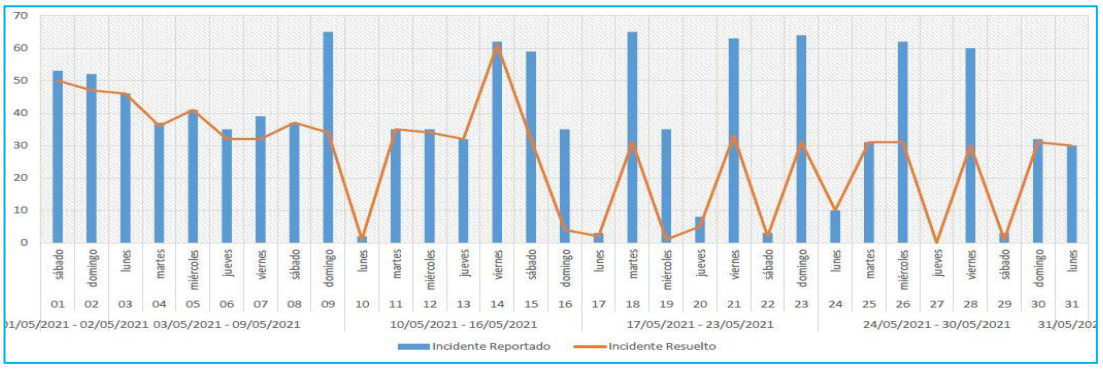

Figura 53 Incidentes resueltos en el mismo día de alerta en el mes de mayo

Fuente: (Royal ITC,2021)

De acuerdo con la Figura presentada anteriormente, se puede observar que la mayoría de los incidentes reportados se resolvieron en el mismo día que fueron alertados; respecto a los eventos alertados y resueltos en el mismo día, se presenta la siguiente figura.

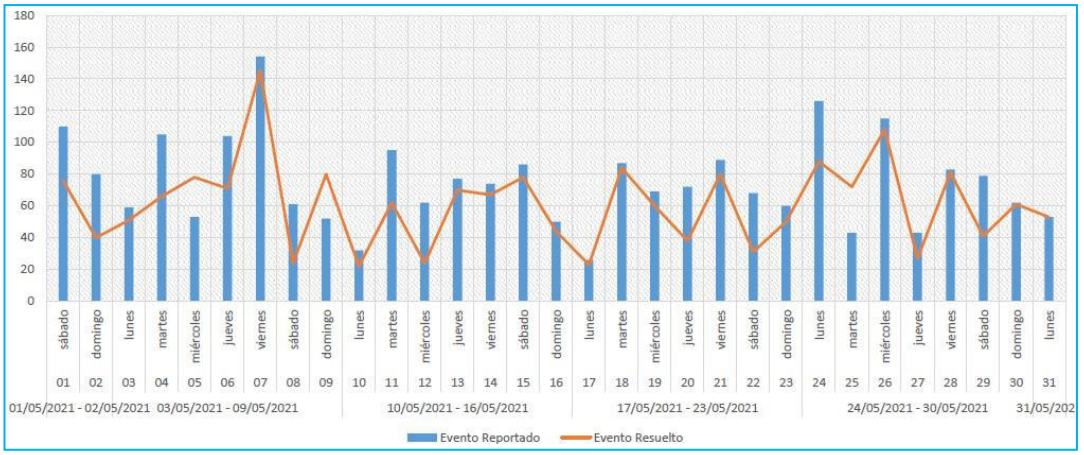

Figura 54 Eventos resueltos en el mismo día de alerta en el mes de mayo

Fuente: (Royal ITC,2021)

Resultados de gestión y correlación de eventos

En la siguiente Figura se puede apreciar la cantidad de eventos por turno para el mes de mayo, donde se puede ver que en promedio los eventos para el mes de mayo fueron 350 durante el turno noche.

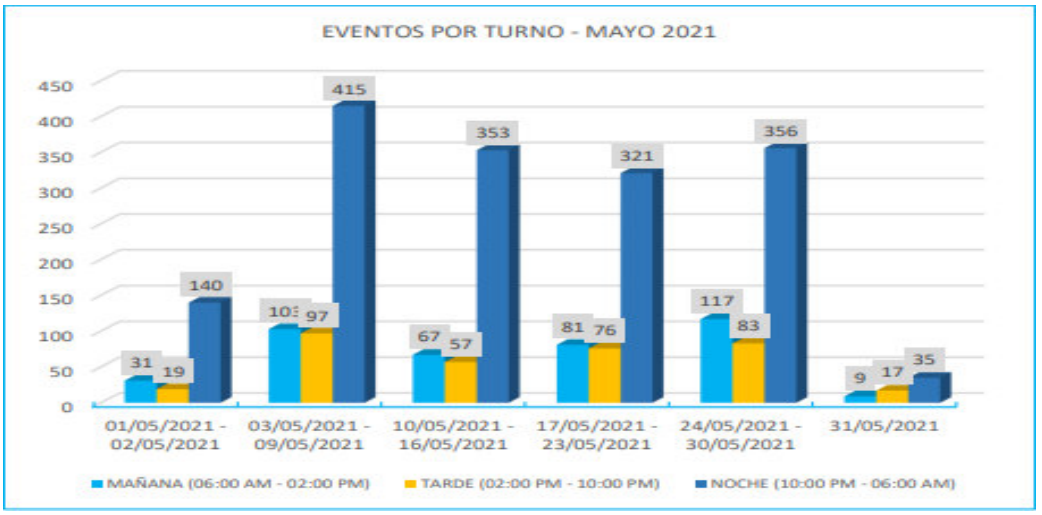

Figura 55 Eventos por turno

Fuente: (Royal ITC,2021)

En la siguiente figura se muestra el número de eventos por nivel criticidad para el mes de mayo, teniendo un total de 2377, siendo 1419 de nivel crítico,146 de nivel alto, 31 de nivel medio y 781 de nivel bajo. En el Anexo 04 se puede visualizar el listado de todos los eventos suscitados durante el mes de mayo

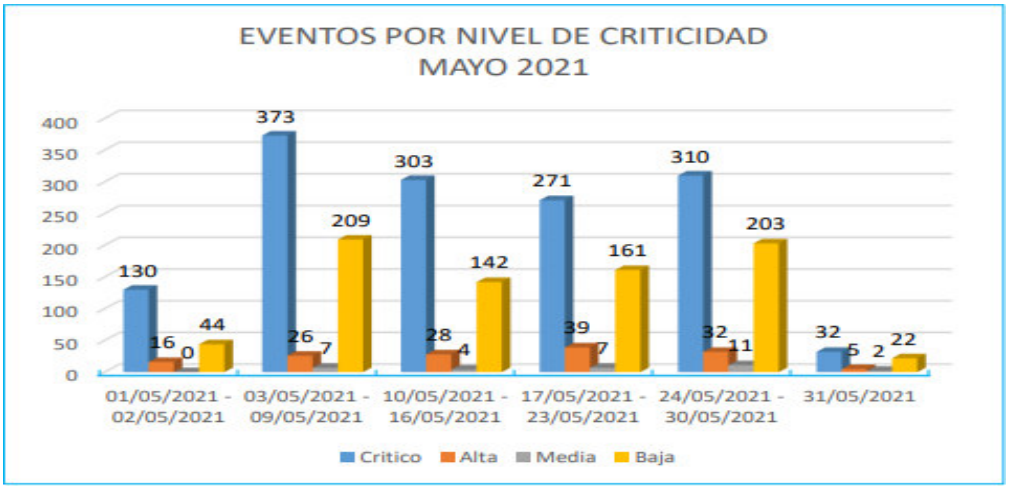

Figura 56 Eventos por nivel de criticidad

Fuente: (Royal ITC,2021)

Resultados de gestión de análisis forense

Durante la aplicación y duración del servicio no se tuvo requerimientos asociados a gestión de análisis forense, por lo que este sub-servicio no se realizó.