Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

Implementación de un sistema de alerta temprana de autenticación para los administradores de sistemas críticos, que permita reportar accesos no autorizados de la empresa de telecomunicaciones y seguridad informática

Proyecto de Titulación

Previo la obtención del Título de:

Magister en seguridad informática

Presentado por:

Ing. German Antonio Valenzuela Franco

Ing. Andrés Mauricio Villavicencio López

Guayaquil - Ecuador

Año: 2026

Dedicatoria

Dedico este trabajo con cariño y gratitud a mis padres, por ser la base de mi formación, por su ejemplo de lucha constante y por enseñarme que con esfuerzo y perseverancia todo es posible.

A mis hermanos, por estar siempre presente, aún en la distancia o el silencio, dándome su apoyo incondicional y creyendo en mí incluso cuando yo dudaba.

Y, sobre todo, a mí mismo, por no rendirme, por mantenerme firme en mis objetivos y por demostrarme que sí podía llegar hasta aquí.

Germán Antonio Valenzuela Franco

Dedicatoria

Dedico este trabajo a mis padres, hermanos y esposa, quienes han sido el soporte y apoye incondicional que me permite alcanzar metas y logros, así como cumplir con el presente trabajo.

Andrés Villavicencio López

Agradecimientos

Agradezco profundamente a Dios por brindarme salud, sabiduría y fortaleza en cada etapa de este proceso académico y personal.

A mis padres, quienes con su ejemplo, esfuerzo incansable y amor incondicional sembraron en mí los valores que me motivaron a seguir adelante, incluso en los momentos más retadores.

A mi compañero de tesis, Andrés Villavicencio, por su compromiso, apoyo mutuo y la sinergia construida durante todo este recorrido.

Germán Antonio Valenzuela Franco

Agradecimientos

Agradezco principalmente a Dios por brindarme las oportunidades diarias.

A mis padres, por el apoyo incondicional a lo largo de mi vida.

A mi esposa por ser el pilar de mi día a día, por el amor y el apoyo moral necesario en el proceso.

A mi compañero de tesis, German Valenzuela, por su esfuerzo y dedicación para afrontar los retos presentado en el proceso.

Andrés Villavicencio López

Declaración Expresa

Nosotros Andrés Mauricio Villavicencio López y Germán Antonio Valenzuela Franco acordamos y reconocemos que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique a los autores que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 17 de enero del 2026.

Firmado electrónicamente por:
GERMAN ANTONIO VALENZUELA FRANCO
Validar únicamente con FirmaEC

Ing. Germán Antonio Valenzuela Franco

Firmado electrónicamente por:
ANDRES MAURICIO VILLAVICENCIO LOPEZ
Validar únicamente con FirmaEC

Ing. Andrés Mauricio Villavicencio López

Evaluadores

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO
Validar únicamente con FirmaEC

MSc. Lenin Eduardo Freire Cobo

Tutor

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA
Validar únicamente con FirmaEC

MSc. Juan Carlos García Plúa

Revisor

Resumen

El objetivo del presente trabajo de titulación es desarrollar un sistema de autenticación de alerta temprana adecuado para los administradores de sistemas críticos en una empresa de telecomunicaciones y seguridad de la información. El objetivo es informar sobre accesos no autorizados y mejorar la seguridad lógica institucional. Se están utilizando herramientas existentes para crear alertas automáticas basadas en eventos de autenticación para patrones de acceso anómalos y una respuesta temprana a posibles problemas de seguridad. Se recopiló información sobre sistemas críticos, registros de eventos y el personal responsable de la administración de los mimos. La implementación involucró la configuración de plataformas SIEM, mecanismos de monitoreo adicionales y su conexión a los sistemas de autenticación existentes. Además, se establecieron los procedimientos de validación para el sistema, pruebas de funcionalidad y documentación para habilitar la funcionalidad del sistema. Las pruebas realizadas en un entorno de laboratorio permitieron evaluar el rendimiento del sistema frente a intentos de acceso no autorizados, cambios de privilegios y accesos fuera de horario, lo que facilitó el ajuste de umbrales y la reducción de falsos positivos. Así, el proyecto ofrece una solución que cumple con el estándar ISO/IEC 27002 y es adecuada para entornos de alta criticidad.

Palabras clave: Seguridad de la información, autenticación, sistemas críticos, alertas tempranas, accesos no autorizados, SIEM.

Abstract

The objective of this thesis is to develop an early warning authentication system suitable for administrators of critical systems in a telecommunications and information security company. The goal is to report unauthorized access and improve institutional logical security. Existing tools are being used to create automatic alerts based on authentication events for anomalous access patterns and to enable early response to potential security issues. Information was gathered on critical systems, event logs, and the personnel responsible for their administration. Implementation involved configuring SIEM platforms, additional monitoring mechanisms, and connecting them to existing authentication systems. Furthermore, system validation procedures, functionality testing, and documentation were established to enable system functionality. Testing in a laboratory environment allowed for the evaluation of system performance against unauthorized access attempts, privilege changes, and after-hours access, facilitating the adjustment of thresholds and the reduction of false positives. Thus, the project offers a solution that complies with the ISO/IEC 27002 standard and is suitable for highly critical environments.

Keywords: Information security, authentication, critical systems, early warnings, unauthorized access, SIEM.

Índice general

Abreviaturas

API	Application Programming Interface
EDR	Endpoint Detection and Response
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LOPDP	Ley Organica de Protección de Datos Personales
MTTD	Mean Time To Detect
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOAR	Security Orchestration, Automation, and Response
TTR	Time To Response
VPN	Virtual Private Network

Simbología

min	Minutos

Índice de figuras

Índice de tablas

Capítulo 1

1.1. Introducción

En la actualidad, el uso de tecnologías digitales forma parte del día a día de las organizaciones, pero también ha aumentado los riesgos asociados a la seguridad de la información. Por esta razón, proteger los datos y los sistemas se ha vuelto una tarea fundamental. En empresas dedicadas a las telecomunicaciones y a la seguridad informática, este cuidado es aún más importante, ya que trabajan con sistemas sensibles y de alto impacto. Un control inadecuado de los accesos puede provocar fallas en la operación, afectar la confianza de usuarios y clientes, y generar problemas legales.

En los últimos años, los problemas de seguridad causados por los accesos no autorizados a los sistemas críticos, han puesto en evidencia la importancia de anticiparse a este tipo de eventos. Cambios como el aumento del trabajo remoto, el uso de dispositivos personales y la necesidad de que los administradores accedan a los sistemas desde distintos lugares han hecho que la verificación de accesos sea más compleja. Como resultado, las medidas de seguridad tradicionales ya no son suficientes para enfrentar estos nuevos escenarios.

Debido a esta situación, este trabajo de titulación se enfoca en la implementación de un sistema de alerta temprana de autenticación. En lugar de proponer cambios complejos o nuevas arquitecturas, la propuesta se basa en aprovechar las herramientas ya disponibles en la organización, configurándolas para detectar accesos inusuales a sistemas críticos.

La propuesta se lleva a cabo en un entorno real,, dentro de una empresa ecuatoriana del sector tecnológico, lo que permite comprobar su utilidad en la práctica y su impacto en la reducción de riesgos relacionados con accesos no autorizados. Para ello, se realiza un análisis de la información disponible, como los registros del sistema, las capacidades de las herramientas de monitoreo ya implementadas y la forma en que trabajan los equipos de infraestructura y seguridad.

Esta introducción sienta las bases del documento, en el que se detallan las etapas de levantamiento de información, configuración técnica, validación funcional y evaluación de resultados, con el propósito de demostrar que una implementación eficiente, basada en buenas prácticas, puede fortalecer la seguridad lógica sin requerir inversiones excesivas ni transformaciones disruptivas.

1.2. Antecedentes

Una empresa de telecomunicaciones y seguridad informática ubicada en la ciudad de guayaquil, que cuenta con más de 25 años de experiencia en el mercado ecuatoriano, brindado servicios de conectividad y seguridad para el sector corporativo, misma que dispone de cuatro mil trabajadores, ha surgido una preocupación crucial relacionada con la seguridad de sus sistemas críticos.

A partir de la pandemia del COVID-19, los controles implementados en los sistemas tuvieron grandes cambios, esto debido a que el perímetro de la red que se enfocaba en los equipos de seguridad y los sistemas en las premisas de la compañía debió ser remplazado por el teletrabajo, con lo cual se volvió necesario el acceso desde redes y equipos fuera del control interno, siendo algunos de ellos equipos personales de los trabajadores, e implantado algunas medidas tales como redes privadas virtuales (VPN, por sus sigla en inglés) y/o detección y repuesta de punto final (EDR, por sus sigla en inglés) para mitigar los riegos.

En diciembre del 2022 se detectó una vulnerabilidad de día cero conocida como log4shell, que puede permitir a los atacantes ejecutar código malicioso de forma remota, la facilidad de explotar la vulnerabilidad y la cantidad de marcas, sistemas o plataformas vulnerables, género en el ecosistema mundial de seguridad gran incertidumbre por el correcto manejo de la superficie de ataque que cada organización y por ende en la empresa de telecomunicaciones y seguridad informática la necesidad de mejorar los controles en sus

sistemas críticos, instalando agentes de colección de logs y de escaneo continuo de vulnerabilidades técnicas.

A pesar de los controles implementados, en la web es posible encontrar a la venta o incluso de forma gratuita conjuntos de credenciales de acceso a diferentes sistemas y organizaciones, estos provienen de navegadores infectados, campañas de phishing, filtraciones de bases de datos, etc. Permitiendo a un atacante atentar contra la confidencialidad, integridad y disponibilidad de la información en las organizaciones.

El detectar y notificar estos hallazgos o los accesos que puedan surgir como consecuencias de las filtraciones, es una preocupación para el departamento de ciberseguridad de la empresa de telecomunicaciones y seguridad informática.

1.3. Descripción del Problema

El personal de ciberseguridad de la empresa de telecomunicaciones y seguridad informática ha identificado en el primer semestre del 2023 aproximadamente 170 filtraciones de credenciales de acceso de diversas plataformas de empresa en la darkweb, lo que representa un riesgo inminente para la integridad y la confidencialidad de la información de la empresa.

Estas credenciales comprometidas brindan a los ciberdelincuentes la oportunidad de acceder de manera fraudulenta a sistemas de alta criticidad utilizando las identidades legítimas de los administradores. Este tipo de acceso no autorizado plantea múltiples amenazas a la organización como pérdida y robo de información, cifrado de sistemas críticos, daño a la reputación, indisponibilidad de servicios, incumplimiento de normativas, entre otros.

La detección y contención de esta incidencia de seguridad toma un tiempo considerable hasta que un administrador pueda reconocer o no la actividad y el departamento

de ciberseguridad pueda tomar las contramedidas correspondientes, inclusive pueden presentarse accesos no autorizados que no sean detectados.

Al implementar un sistema de alerta temprana de autenticación, se mejoraría significativamente la capacidad de la empresa para detectar y responder de manera oportuna a los accesos no autorizados, lo que, a su vez, reduciría los riesgos y las consecuencias negativas de los ciberataques. [1]

Los autores de la presente propuesta laboran dentro del departamento de ciberseguridad por lo cual están inmersos en la problemática diariamente, frente a la cual la alta gerencia ha solicitado al departamento implementar medidas de control. Los autores disponen de acceso a las herramientas, licenciamientos necesarios para abarcar una solución y adicional se tienen contacto directo con la mayoría de los administradores de sistemas críticos, esto permite implementar la solución propuesta en un tiempo aproximado de 4 meses.

1.4. Solución Propuesta

En este contexto, se utilizará herramientas de gestión de la información y eventos de seguridad (SIEM, por sus siglas en ingles) para la correlación de logs provenientes de los sistemas críticos que permitan la generación de alertas tempranas, para la integración con el sistema de orquestación de seguridad, automatización y respuesta (SOAR, por sus siglas en inglés) y notificación al administrador mediante mensajería instantánea, quién a su vez puede reportar inmediatamente un acceso no autorizado al personal de ciberseguridad. [2] [3]

La ventaja de esta solución es una rápida interacción entre el grupo dedicado a la ciberseguridad de la compañía y los administradores de sistemas críticos, permitiendo cumplir las normativas y regulaciones tales como la ley orgánica de protección de datos personales, ley orgánica de telecomunicaciones, etc. [4]

El departamento de ciberseguridad, ha implementado controles a fin de minimizar la fugas de credenciales como bloqueo de almacenamiento de credenciales en navegadores web, implementación de detección y repuesta de punto final (EDR, por sus siglas en ingles) y sistemas antispam, sin embargo, no es posible cerrar completamente las brechas de seguridad, por ello es necesario aplicar un sistema que ayude a identificar los accesos no autorizados que puedan ocurrir como consecuencia de las filtraciones, mismas que pueden ser publicadas en plataformas web, grupos de redes sociales y puestas en venta como paquetes de información. [5]

Con el sistema propuesto, el administrador podrá identificar cuando un acceso no corresponde a las actividades laborales que desempeña, por lo cual se debe accionar los planes de repuesta ante incidentes que mantiene la empresa con el departamento de ciberseguridad. Por lo antes mencionado, la implementación de un sistema de alerta temprana es la adecuada solución para el remanente de la brecha de seguridad y de apoyo a la empresa.

1.5. Objetivos

1.5.1. Objetivo General

Implementar un sistema de alerta temprana de autenticación anómala en sistemas críticos para los administradores y personal de ciberseguridad de una empresa de telecomunicaciones y seguridad informática, utilizando tecnologías SIEM y SOAR integrando una aplicación de mensajería instantánea.

1.5.2. Objetivos Específicos

- Preparar datos de sistemas críticos, su infraestructura y sus patrones anómalos de acceso.
- Configurar reglas de detección en la plataforma SIEM.
- Implementar una plataforma SOAR para orquestar, automatizar y notificar las respuestas de las alertas generadas por el SIEM.

1.6. Metodología

El estudio es de naturaleza no experimental y transversal debido a que implica la ejecución de una intervención controlada alertando a los administradores. A través del diseño, los autores podrán recopilar datos sistemáticos antes y después de la implementación del sistema para analizar si este ha tenido un efecto significativo en la seguridad de los sistemas críticos.

En el presente estudio se efectuará un muestreo no probabilístico basado en conveniencia, los autores laboran en el departamento de seguridad lógica de la empresa de telecomunicaciones y seguridad informática, por sus actividades conocen la información de sistemas establecidos como críticos y mantiene interacción con tres departamentos con el mayor número de estos sistemas.

Se implementará la técnica de Focus Group con administradores de 3 departamentos con mayor número de sistemas críticos y coordinación del equipo de monitoreo de ciberseguridad, que incluye una entrevista a realizarse de forma virtual por una plataforma de videoconferencia.

Durante el Focus Group, se incorporarán 10 preguntas enfocado a la experiencia, necesidad y preferencia de los administradores y equipo de monitoreo de ciberseguridad respecto a la identificación de los accesos, así como la forma de notificar las incidencias, con el objetivo de obtener información cualitativa y perspectiva de cómo se trata actualmente este tipo de incidencias y cuáles son acciones para aplicar.

Se efectuará un análisis estadístico de la información recolectada en la entrevista, con lo que se espera obtener información como la aplicación de mensajería instantánea preferida, equipo de monitoreo de seguridad para la notificación de alertas, tiempo de notificación y otras acciones automatizadas que se puedan ejecutar como una respuesta ante incidente.

Para inventariar los activos que intervendrán en el sistema de alerta temprana, se procede a obtener un reporte de activos categorizados como críticos del aplicativo de inventario administrado por el departamento de ciberseguridad, que incluya el nombre del activo, direcciones IPs, administrador y los agentes de monitoreo instalados. Esta información deberá ser complementada con los contactos de los administradores, para ello se implementará un formulario mediante correo electrónico.

Aquellos activos que no cuenten con los agentes de monitoreo, se realizará un seguimiento con el departamento de ciberseguridad, para asegurar la instalación de agentes y las configuraciones de almacenamiento de logs necesarios para el sistema.

Para generar las alertas en el SIEM, se crearán los casos de uso con las respectivas reglas de correlación de logs, que permitan identificar los posibles accesos no autorizados a los sistemas monitoreados. Las alertas serán enviadas mediante interfaz de programación de aplicaciones (API, por sus siglas en inglés) al sistema SOAR, en el cual se implementará un flujo de procesos automatizado encargado de añadir datos adicionales a la alerta y notificar mediante una aplicación de mensajería instantánea al administrador, quien tendrá la opción de reconocer la actividad como propia de sus labores o como un acceso no autorizado y mediante la misma aplicación de mensajería instantánea, notificar al departamento de ciberseguridad para gestionar la respuesta al incidente correspondiente. [6]

Con la información recopilada, se deberá efectuar una segunda sesión con la jefatura y/o gerencia del departamento de ciberseguridad para presentar la propuesta y recibir posibles cambios, mejoras o nuevos requerimientos sobre el proyecto.

1.6.1. Focus group

El focus group propuesto se compone de 9 participantes de los cuales 6 son administradores de sistemas críticos (2 por cada departamento considerado previamente), 1

especialista y 1 coordinador de monitoreo de ciberseguridad, así como, 1 ingeniero de automatización.

El guion para el focus group es validado por la jefatura del departamento de monitoreo de ciberseguridad y está compuesto por las siguientes preguntas:

- Cuando ocurre una actividad inusual en el sistema (por ejemplo, accesos fuera de horario), ¿recibe algún tipo de aviso o notificación?
- ¿Cómo suele enterarse cuando alguien accede a los sistemas que usted administra? (Ej.: correos, llamadas, herramientas, no se entera, etc.)
- Desde su experiencia, ¿en cuánto tiempo suele enterarse de este tipo de situaciones después de que ocurren?
- ¿Qué dificultades ha tenido para identificar si una actividad fue realizada por usted, su equipo o por otra persona?
- ¿Qué mensajería instantánea considera más práctico y rápido para recibir alertas importantes sobre sus sistemas? (Ej.: Whastapp, Telegram, Line, otros)
- Cuando recibe una alerta o aviso, ¿qué tan claro le resulta saber qué ocurrió y qué acción debería tomar?
- En caso de detectar o sospechar un acceso no autorizado, ¿qué acciones suele realizar y a quién notifica?
- ¿Qué tareas relacionadas con la revisión de accesos o notificaciones considera que podrían realizarse de forma automática para facilitar su trabajo?
- ¿Cómo cree que cambiaría su forma de trabajo si recibiera alertas inmediatas sobre accesos inusuales a sus sistemas?
- Describa que tan frecuente realiza cambios en los sistemas fuera de horario laboral.

Como resultado del focus group se identificó que la mensajería instantánea ideal es Telegram, por su uso interno en la empresa y que tanto los administradores como el personal de monitores de ciberseguridad cuentan con número corporativos. Se identificó que la revisión de accesos sospechas y el tiempo de resolución toma incluso días, esto debido al uso del correo como medio de notificación, el cual la mayoría del personal lo revisa solo en horario de oficina.

1.6.2. Criterio de éxito

Con el presente proyecto se espera obtener los criterios definidos en la tabla 1 para considera una implementación exitosa.

Tabla 1

Criterios de éxito

Indicador	Criterio de éxito
MTTD (min)	Reducción ≥ 30%
TTR (min)	Reducción ≥ 25%
Falsos Positivos (%)	≤ 20% del total de alertas
Eventos anómalos detectados (%)	Incremento ≥ 20%
SLA cumplidos (%)	≥ 95%

.

Capítulo 2

2. Marco teórico

El presente trabajo se aborda la necesidad de mejorar la detección y respuesta ante accesos no autorizados a sistemas críticos por parte de administradores de sistemas. La implementación de un sistema de alerta temprana de autenticación se propone como una solución para reducir el tiempo de respuesta y mitigar los riesgos asociados con estas violaciones de seguridad. A continuación, se incorporan las siguientes definiciones y conceptos:

2.1. Seguridad de la información

La seguridad de la información engloba el conjunto de medidas destinadas a salvaguardar la confidencialidad, integridad y disponibilidad de los datos frente a diversas amenazas y riesgos. Este enfoque busca garantizar la preservación de la información, evitando su acceso no autorizado, asegurando su exactitud y fiabilidad, y manteniendo la accesibilidad cuando sea necesaria, con el propósito fundamental de resguardar la integridad y el buen funcionamiento de los sistemas de información. [7]

Los tres pilares fundamentales de la seguridad de la información conocidas también como la triada CIA se pueden observar en representación gráfica en la Figura 1 y se presentan a continuación:

Figura 1

Triada CIA

Fuente: https://ciberseguridadcrimiceu.blogspot.com/2021/04/modelo-de-seguridad-cia.html

- **Confidencialidad:** Tiene como finalidad prevenir la revelación no autorizada de los datos. Esto quiere decir que la información solo puede ser accesible para las personas, sistemas o procesos que cuentan con los permisos correspondientes, evitando el uso o divulgación indebida. [8]
- **Integridad:** Se refiere a que la información debe mantenerse precisa y correcta. Esto quiere decir que los datos no deben ser manipulados sin autorización y que cualquier cambio esté debidamente controlado. [8]
- **Disponibilidad:** Es el principio que garantiza que los sistemas y la información sean accesibles en el momento en que un usuario los requiera, asegurando la continuidad de la operación del negocio. Para lograr este principio se puede implementar medidas como redundancia, respaldos, mantenimientos, entre otros. [8]
- **Activo de información**: Comprende elementos que sean de importancia para la empresa, que se usan o generan en sus operaciones. Abarca una amplia variedad de formas, desde datos y documentos hasta sistemas y procesos críticos. Por su importancia la empresa debe resguárdalos y aplicar la triada de la CIA. [8]
- **Autenticación:** Es el proceso mediante el cual se verifica la identidad de un individuo o un objeto, es decir confirmar de manera segura y fiable que la entidad en cuestión es quien afirma ser, asegurando la legitimidad de las interacciones en entornos diversos, donde la certificación de identidad desempeña un papel fundamental para proteger la integridad y confianza en los sistemas y servicios. [7]
- **Autorización:** La autorización comprende el procedimiento mediante el cual se concede o niega el acceso a recursos particulares o la ejecución de acciones específicas, basándose en roles o identidades predefinidos. Este proceso es esencial para establecer controles de seguridad, ya que determina qué usuarios o entidades

tienen el privilegio de acceder a determinados recursos o llevar a cabo ciertas operaciones. Al implementar la autorización, se busca no solo salvaguardar la confidencialidad, integridad y disponibilidad de los datos, sino también gestionar de manera eficaz los permisos y privilegios dentro de un sistema, contribuyendo así a un entorno informático más seguro y gestionado. [7] [9] [10]

- **Control de accesos:** Es un conjunto de medidas que permiten regular quién puede acceder a los sistemas, datos o espacios, y qué acciones puede realizar dentro de ellos. Su objetivo es asegurar que solo las personas o procesos autorizados tengan acceso a los recursos de la organización. [7]
- **Ataque:** Un ataque se define como un intento malicioso dirigido a dañar o comprometer sistemas o datos, con la intención de obtener acceso no autorizado, manipular información o interrumpir el funcionamiento normal de los recursos. Este acto perjudicial puede manifestarse de diversas formas, desde intrusiones informáticas hasta la explotación de vulnerabilidades, y tiene como objetivo primordial el menoscabo de la integridad, confidencialidad o disponibilidad de la información. La identificación y comprensión de posibles ataques son esenciales para el desarrollo de estrategias de seguridad efectivas, con el propósito de prevenir y mitigar los riesgos asociados a estas amenazas maliciosas en entornos digitales y de tecnologías de la información. [9] [10]
- **Consecuencia:** Una consecuencia se refiere al resultado o efecto que se deriva de una acción, decisión o evento específico. Este término implica la conexión directa entre una causa y su impacto, representando la manifestación tangible o lógica de lo que sigue a una determinada situación. Las consecuencias pueden abarcar una amplia gama de aspectos, desde resultados positivos hasta desenlaces negativos, y su comprensión es esencial para evaluar las implicaciones y ramificaciones de diversas

acciones o circunstancias. En contextos como la seguridad de la información, la identificación y gestión adecuada de las consecuencias se convierten en elementos cruciales para la toma de decisiones informadas y la mitigación de posibles riesgos. [7]

- **Seguridad informática:** La seguridad informática se ocupa de proteger sistemas, datos y redes contra amenazas y riesgos cibernéticos. Su ámbito de acción incluye la implementación de tecnologías, políticas y prácticas diseñadas para fortalecer la integridad, confidencialidad y disponibilidad de la información. Abarca un enfoque integral para resguardar la infraestructura tecnológica, detectar y responder a posibles ataques, y garantizar la continuidad operativa en un entorno digital en constante evolución. [11]
- **Ciberseguridad:** Ciberseguridad aborda la salvaguardia de sistemas digitales, redes y datos contra diversas amenazas, ataques y vulnerabilidades en el entorno digital. Su enfoque principal es preservar la integridad, confidencialidad y disponibilidad de la información, empleando medidas y estrategias específicas para contrarrestar los desafíos emergentes y dinámicos del ciberespacio. [9] [12]
    - **Herramientas:** Las herramientas de ciberseguridad son software o dispositivos que se utilizan para proteger sistemas, redes y datos contra amenazas y riesgos cibernéticos. Estas herramientas ayudan a identificar, prevenir, mitigar y responder a ataques informáticos y otras vulnerabilidades de seguridad como: Firewalls, Antivirus, IDS, IPS, 2FA, IAM, etc. [9] [10]

2.2. Sistema de alerta de autenticación

Un Sistema de Alerta de Autenticación se configura como una herramienta especializada que tiene la capacidad de identificar y comunicar cualquier intento de inicio de

sesión que se perciba como inusual o sospechoso en un sistema determinado. Su función principal radica en salvaguardar la seguridad de las cuentas y sistemas, proporcionando una capa adicional de defensa al alertar proactivamente sobre posibles amenazas o actividades no autorizadas en el proceso de autenticación. Este sistema contribuye significativamente a la detección temprana de potenciales riesgos de seguridad, permitiendo una respuesta rápida y eficaz para mitigar posibles vulnerabilidades y proteger la integridad de las credenciales y la información almacenada. [10]

- **Sistemas de detección de intrusos (IDS):** Los Sistemas de Detección de Intrusos (IDS) son herramientas especializadas que realizan una vigilancia constante y emiten alertas ante intentos de autenticación que son considerados no autorizados o que muestran comportamientos anómalos en una red o sistema específico. Estos sistemas desempeñan un papel crucial en la identificación temprana de actividades sospechosas, contribuyendo a la protección de la seguridad de la red al detectar posibles amenazas o intrusiones. Al monitorear de manera proactiva los eventos relacionados con la autenticación, los IDS permiten una respuesta rápida y efectiva ante posibles violaciones de seguridad, mejorando así la resiliencia y la integridad del entorno informático. [9], [10]
- **Sistemas de prevención de intrusos (IPS):** Los Sistemas de Prevención de Intrusos (IPS) no solo tienen la capacidad de alertar ante intentos de autenticación maliciosos o no autorizados, sino que también pueden llevar a cabo acciones automáticas para bloquear dichos intentos. Estos sistemas se caracterizan por su funcionalidad proactiva, ya que no se limitan a la detección y notificación, sino que implementan medidas preventivas inmediatas en tiempo real. Al identificar patrones o comportamientos anómalos en los intentos de autenticación, los IPS toman medidas para bloquear o mitigar automáticamente las amenazas, contribuyendo así a reforzar

la seguridad del sistema y prevenir posibles intrusiones antes de que puedan causar daño o comprometer la integridad de la red. [9], [10]

- **Autenticación de dos factores (2FA):** La Autenticación de Dos Factores (2FA) es un sistema que demanda, además de la contraseña convencional, una segunda forma de autenticación. Esta segunda capa de verificación puede tomar la forma de un código generado por una aplicación específica o un token de seguridad. La incorporación de este segundo factor fortalece significativamente la seguridad del proceso de autenticación, ya que la probabilidad de acceso no autorizado se reduce considerablemente. La 2FA añade una capa adicional de protección, ya que un atacante necesitaría tanto la contraseña conocida como el elemento adicional de autenticación, que suele ser temporal y específico para cada sesión. Este enfoque contribuye de manera efectiva a mitigar el riesgo de accesos no autorizados y a fortalecer la seguridad en la autenticación de usuarios. [9], [10]
- **Herramientas de monitoreo de registros de eventos de seguridad (SIEM):** Las Herramientas de Monitoreo de Registros de Eventos de Seguridad, conocidas como Sistemas de Información y Gestión de Eventos de Seguridad (SIEM), tienen la capacidad de correlacionar eventos de autenticación y generar alertas ante patrones de acceso que se consideran sospechosos. Estas herramientas integran y analizan registros de eventos provenientes de diversas fuentes dentro de un entorno informático, incluyendo actividades de autenticación. Al realizar esta correlación, los SIEM pueden identificar relaciones y contextos entre eventos de autenticación, permitiendo la detección temprana de comportamientos anómalos o potencialmente maliciosos. La capacidad de alertar sobre patrones de acceso sospechosos mejora la capacidad de respuesta ante posibles amenazas, contribuyendo a fortalecer la seguridad global del sistema. [9], [10]

2.3. Sistemas críticos

En el ámbito de la ciberseguridad, los sistemas críticos hacen referencia a activos o infraestructuras esenciales que, en caso de ser comprometidos o experimentar una falla debido a un ataque cibernético, tendrían consecuencias significativas en términos de seguridad nacional, economía o seguridad pública. Estos sistemas son vitales para el funcionamiento continuo y la estabilidad de una nación, y su compromiso podría resultar en efectos adversos a gran escala. La protección de los sistemas críticos se convierte en una prioridad estratégica en la ciberseguridad, ya que su integridad y disponibilidad son fundamentales para el bienestar y la seguridad a nivel nacional. [13], [14]

- **Importancia estratégica:** El sistema es fundamental para el funcionamiento de la organización o para cumplir con sus objetivos estratégicos. Su interrupción o compromiso tendría un impacto significativo en la organización.
- **Relevancia para la seguridad pública:** El sistema está relacionado con la seguridad pública, la salud y la seguridad de las personas, la protección del medio ambiente o la seguridad nacional.
- **Interdependencia:** El sistema está interconectado con otros sistemas y depende de ellos, o bien, otros sistemas dependen de él. Su fallo podría tener un efecto dominó en otras áreas críticas.
- **Potencial de daño:** La falla o el compromiso del sistema podría resultar en consecuencias graves, como la pérdida de vidas, la interrupción de servicios esenciales o daños significativos a la propiedad.

- **Regulaciones y normativas:** El sistema está sujeto a regulaciones y normativas específicas que establecen requisitos de seguridad y protección para garantizar su funcionamiento adecuado.

2.4. Cumplimiento normativo

La empresa de telecomunicaciones y seguridad de la información esta sujeta a normativas legales y de cumplimento estratégico, en este caso la Ley Orgánica de protección de Datos (LOPDP) y la normativa ISO/IEC 27001 con al cuales se define la gestión de logs de autenticación, la retención y trazabilidad de los mismos. [4], [9]

- Privacidad de los datos: Los logs de autenticación contienen datos personales tales como usuarios, IPs, estampas de tiempo, entre otros, que son usados por los miembros del equipo de monitoreo de ciberseguridad con la finalidad de prevenir incidentes.
- Retención de logs: Las normativas vigentes en la empresa de telecomunicaciones y seguridad de la información implican que los logs deben ser mantenidos por 12 meses, para garantizar que se puedan investigar acciones o incidentes que tengan origen en dicho periodo. [9]
- Control de accesos (ACL) a los logs: Según las normativas debe existir un control de acceso a los registros permitiendo que solo aquel personal con que por sus funciones lo requiere y que los accesos estén basados en los mínimos privilegios posibles. [4]
- Trazabilidad y auditoría: Los mecanismos de trazabilidad aseguran la integridad y confidencialidad de los registros, que pueden ser utilizados en investigaciones o auditorías garantizando el no repudio, alineado con la normativa ISO/IEC 27001.

Capítulo 3

3. Preparación de datos de sistemas críticos

3.1. Inventario de los sistemas críticos, sus administradores y contactos.

Para todo sistema de gestión de seguridad de la información (SGSI) es vital identificar los diferentes activos que forman parte de la empresa y sus características principales, tales como, Hostname, Dirección IP, Criticidad, Custodio de Activo, etc.

Para el presente proyecto se toman en cuenta tres departamentos de la empresa de telecomunicaciones y ciberseguridad, utilizando el sistema de inventario interno de activos de información. Uno de los campos del sistema es criticidad el cual consta de tres niveles alto, medio, bajo, dichos niveles fueron definidos en base a una matriz de riegos, la cual considera el impacto en la disponibilidad de servicios que pueden observar en la Tabla 2 y la probabilidad de ocurrencia, mismo que se pueden observar en la Tabla 3. Estos factores se correlacionan en mapa de calor de la Figura 2, dando como resultado la criticidad del activo.

Tabla 2

Criterio de impacto por fallas en la infraestructura de red, errores técnicos o ataques cibernéticos

Disponibilidad del servicio	**Afectación del servicio**
ALTA	La interrupción afecta a la totalidad o a la mayoría de los usuarios o servicios críticos de la empresa.
MEDIA	La interrupción afecta a un grupo considerable de usuarios o servicios críticos de la empresa.
BAJA	La interrupción afecta a un número limitado de usuarios o servicios no críticos de la empresa.

Fuente: SGSI de la empresa de Telecomunicaciones y ciberseguridad

Tabla 3

Criterio de probabilidad

Probabilidad	Retrospectiva	Prospectiva	Descriptiva
ALTA	Se conoce un factor de ocurrencia en el último trimestre.	Posiblemente se presente una ocurrencia en el próximo trimestre.	El evento o situación de riesgo es altamente probable de ocurrir.
MEDIA	Se conoce un factor de ocurrencia en el último año.	Posiblemente se presente una ocurrencia en el próximo año.	Existe una probabilidad considerable de que el evento o situación de riesgo ocurra en determinadas circunstancias.
BAJA	Se conoce un factor de ocurrencia en los últimos 2 años.	Posiblemente se presente una ocurrencia en los próximos 2 años	Existe una pequeña posibilidad de que el evento o situación de riesgo ocurra.

Fuente: SGSI de la empresa de Telecomunicaciones y ciberseguridad

Figura 2

Mapa de calor

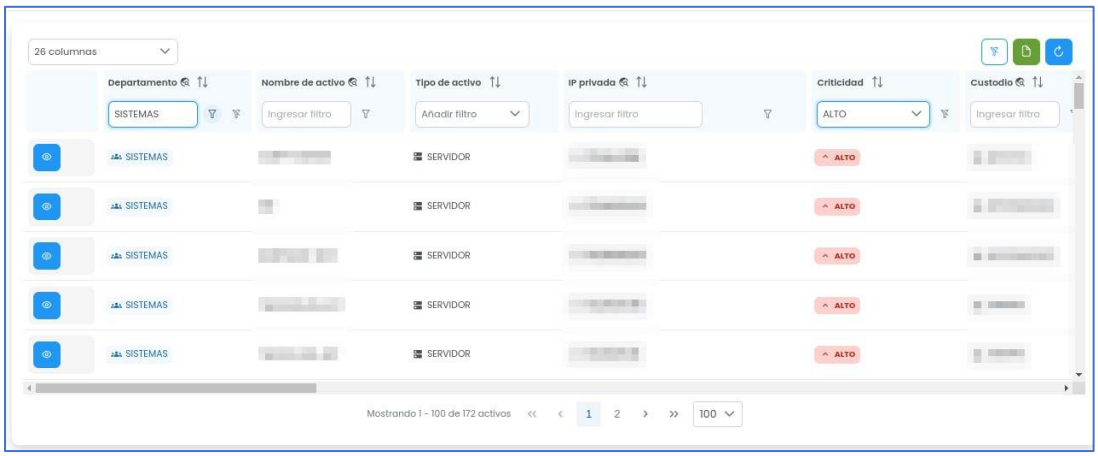
Fuente: SGSI de la empresa de Telecomunicaciones y ciberseguridad

Los tres departamentos tomados en cuenta para el proyecto son: Sistemas, Tecnología de la información y Ciberseguridad.

En la Figura 3 de observa el inventario de activos internos para el departamento de sistemas.

Figura 3

Inventario del departamento "Sistemas"

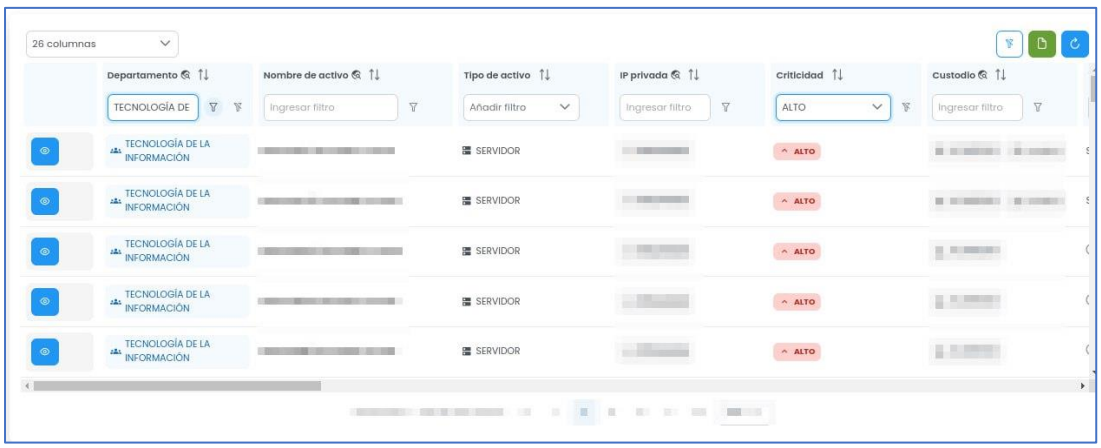


Fuente: Inventario interno de la empresa de Telecomunicaciones y ciberseguridad

En la Figura 4 de observa el inventario de activos internos para el departamento de tecnologías de la información.

Figura 4

Inventario del departamento "Tecnología de la información"

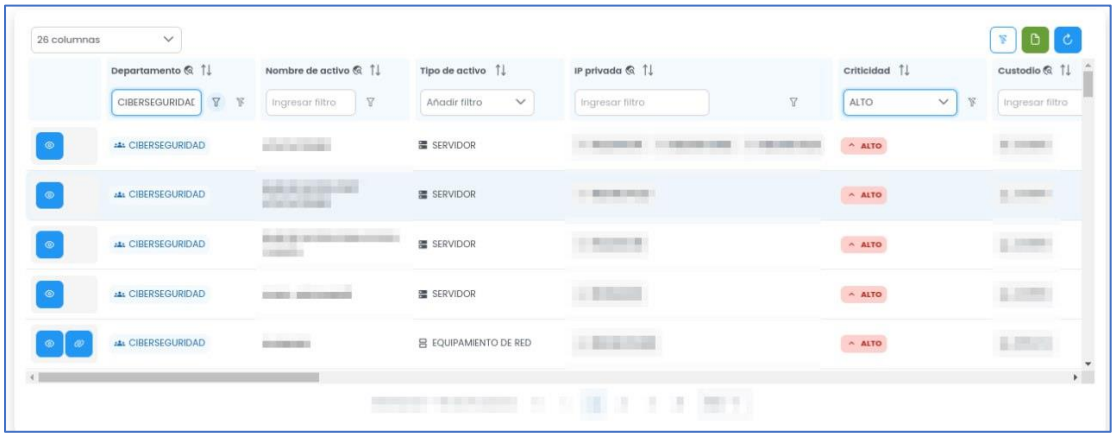


Fuente: Inventario interno de la empresa de Telecomunicaciones y ciberseguridad

En la Figura 5 de observa el inventario de activos internos para el departamento de ciberseguridad.

Figura 5

Inventario del departamento ciberseguridad



Fuente: Inventario interno de la empresa de Telecomunicaciones y ciberseguridad

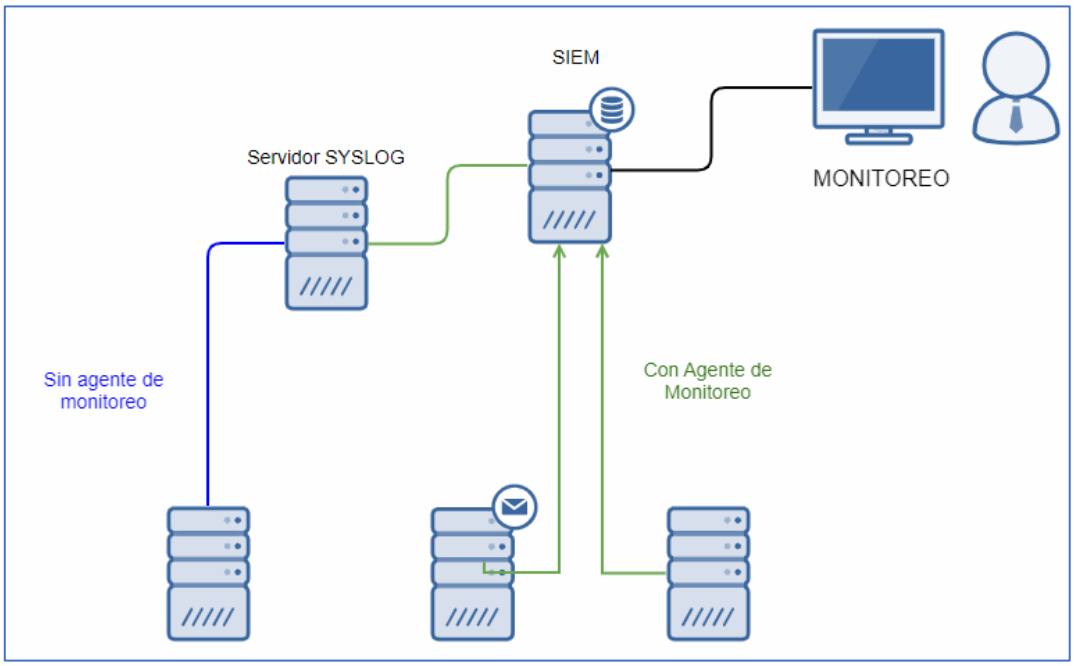
3.2. Gestión de la infraestructura de los sistemas críticos y almacenamiento de logs

Hoy en día el monitoreo de ciberseguridad representa un punto crucial en toda empresa, ante las nuevas vulnerabilidades y amenazas que se presenta diariamente, para lo cual se debe contar con una plataforma que permita centralizar el almacenamiento y análisis de logs de los activos de información para generar las alerta y respuestas ante incidentes respectivas.

La empresa de telecomunicaciones y ciberseguridad en al que se implementa el presente proyecto cuenta con una plataforma SIEM de la marca SPLUNK, cuya arquitectura para la colección, almacenamiento y análisis de logs se muestra en la Figura 6.

Figura 6

Arquitectura para la colección de logs



Fuente: Diagrama de arquitectura del SIEM de la empresa de telecomunicaciones y seguridad de la información.

La arquitectura cuenta con dos métodos para recibir logs, mediante un agente instalado en cada servidor, el cual envía los logs directamente al SIEM o mediante el protocolo syslog. En el caso de aquellos activos que no pueden instalar el agente se tiene un servidor syslog, que recibe los logs de dichos activos y renvía los logs al SIEM mediante el agente splunk heavy forwarder instalado en el mismo.

Con las dos opciones para el envío de logs planteadas todos los activos inventariados pueden centralizar sus logs, evitando la perdida por manipulación de un atacante o por recursos de disco en los propios activos, sin embargo, esto representa un alto costo en recurso para la plataforma SIEM que debe asumir la empresa.

3.3. Identificación de patrones anómalos de accesos a los sistemas

Para establecer los patrones anómalos o sospechosos en los eventos de acceso a un activo crítico se realizó un focus group con personal de los tres departamentos involucrados, en el cual se definió las siguientes reglas:

- Accesos fuera del horario de oficina (8h00 a 18h00) se debe considerar sospechosos, a pesar de que las ventanas de trabajo por actualizaciones o cambios se deban realizar en dichos horarios, los mismo deben ser comunicados con anticipación
- La empresa de Telecomunicaciones y ciberseguridad cuenta con políticas de acceso dentro de su SGSI en las cuales especifica que todo acceso a los sistemas críticos debe realizarse desde una red privada virtual (VPN, por sus siglas en inglés) o desde una red interna de la organización, por lo que cualquier acceso fuera de estas redes es anómalo.
- Los accesos que se presenten posterior a tres intentos fallidos con el usuario se consideran anómalos y deben ser reportados.

Capítulo 4

4. Definición y configuración de reglas de detección en la plataforma SIEM

La plataforma SIEM permite analizar logs, correlacionar logs de diferentes fuentes y generar alertas, mismas que pueden enviarse por correo, mediante mensajería instantánea, a plataformas de orquestación (SOAR), etc.

4.1. Adquisición de logs de autenticación de los sistemas críticos

En base a la arquitectura presentada en la Ilustración 5, los activos tienen dos opciones para enviar logs a la plataforma SIEM, sin embargo, para que dichos logs puedan almacenarse y posteriormente ser utilizados para el análisis y generación de alertas es necesario realizar configuraciones de stanzas. Las stanzas son pequeñas porciones que código que se configuran en la interfaz de administración del SIEM, con las cuales se indica a los activos que tiene un agente instalado que tipo de logs o rutas serán indexadas a la plataforma.

Para el actual proyecto se requiere tener logs de autenticación de los diferentes activos críticos, para lo cual se define las siguientes stanzas:

- Stanza para logs de sistema operativo Linux

```
[monitor:///var/log/auth.log]
disabled = false
index = index-auth-criticos
sourcetype = linux_auth
```

- Stanza para logs de sistema operativo Windows

```
[monitor://C:\Windows\System32\winevt\Logs\Security.evtx]
disabled = false
index = index-auth-criticos
sourcetype = win_security
```

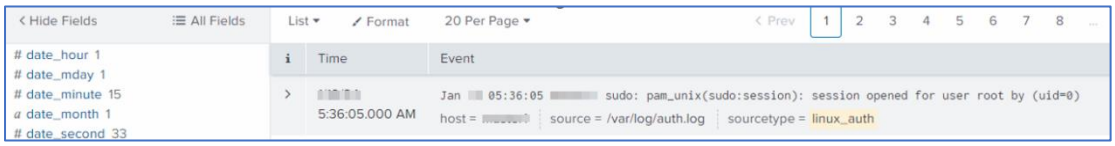
- Stanza para logs recibidos por syslog

```
[monitor: ///var/log/activos_criticos/auth_criticos.log]
disabled = false
index = index-auth-criticos
sourcetype = linux_auth
```

Con las stanzas configuradas y con las instrucciones enviadas a los diferentes servidores se pueden observar logs en la plataforma SIEM, un ejemplo de log de autenticación se puede observar en la Figura 7.

Figura 7

Logs de autenticación en la plataforma SIEM



Fuente: SIEM de la empresa de Telecomunicaciones y ciberseguridad

4.2. Configuración de reglas de detección en plataforma SIEM.

Una vez que se dispone de logs en el SIEM Splunk y tomando en consideración los patrones anómalos definidos se procede a generar una regla de correlación que permita alertar el comportamiento. Se definen 3 regla de correlación:

- Regla basada en horario de acceso

```
| tstats count where (index= index-auth-criticos
(sourcetype=win_security OR sourcetype=linux_auth) action=login
OR action=logout) by sourcetype, _time span=5m
| where (sourcetype=win_security OR sourcetype=linux_auth) AND
(action=login OR action=logout)
| where (strftime(_time, "%H") >= "18" OR strftime(_time, "%H")
< "07")
| table _time, host, username, action
```

- Regla basada en redes externas

```
index= index-auth-criticos
(sourcetype=win_security OR sourcetype=linux_auth) AND
(action=login OR action=logout) NOT src_ip IN (192.168.0.*,
172.29.0.*, 181.198.10*)
| table _time, host, username, action
```

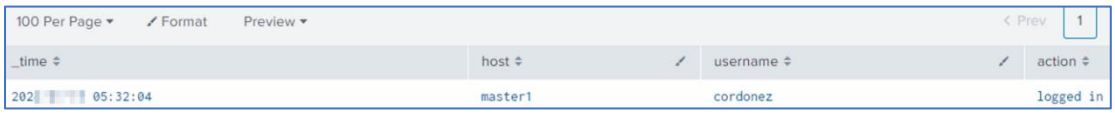
- Regla basada en intentos fallidos

```
index= index-auth-criticos
(sourcetype=win_security OR sourcetype=linux_auth)
AND action=failed_login
| stats count by host, user, _time
| where count > 3 by host, user
| table _time, host, username, action
```

Adicional se configura para una vez generada la alerta se envíe una notificación por correo electrónico a al equipo de ciberseguridad, así mismo por medio de un webhook se envía a la plataforma SOAR para la automatización de notificación al custodio del activo alertado. Como parte del piloto ejecutado en la Figura 8 se puede observar una alerta generada por el sistema.

Figura 8

Alerta generada en el SIEM por horario



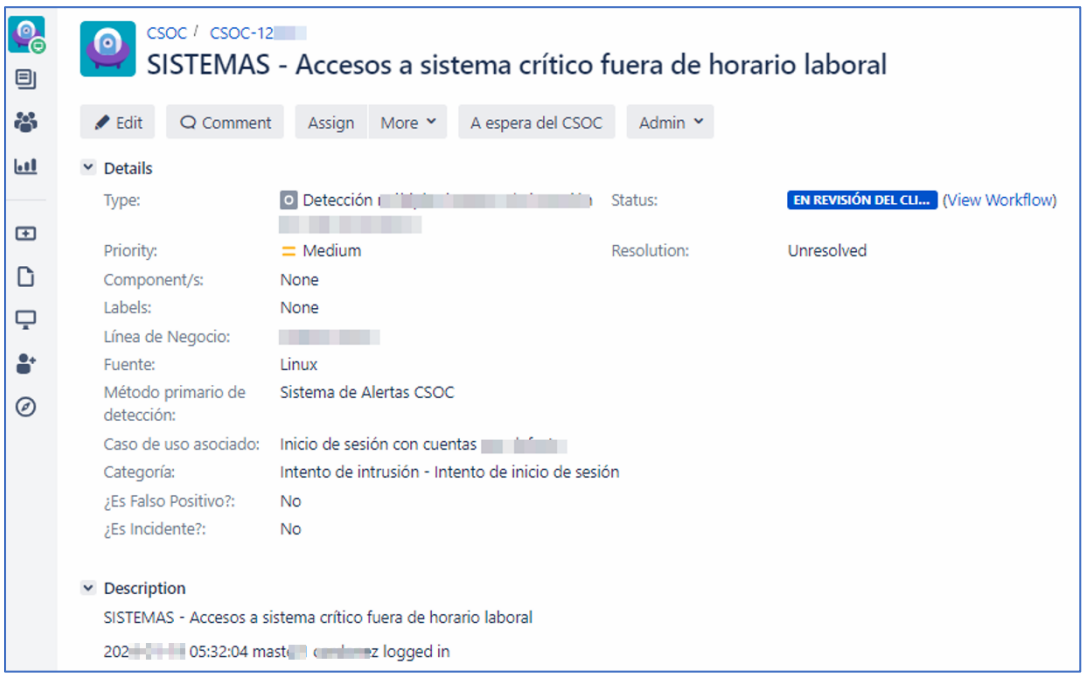
Fuente: SIEM de la empresa de Telecomunicaciones y ciberseguridad

4.3. Definición del proceso del registro de alertas en ticketera

Toda alerta generada desde el SIEM debe generar un ticket en la plataforma de tickets interna del equipo de ciberseguridad, para ello el SIEM enviará por medio de webhook los datos de la alerta hacia la ticketera y está generará un ticket, que quedará en un estado pendiente de usuario, hasta recibir la confirmación de acceso valido o reporte de acceso no autorizado por parte del custodio, continuando con el piloto ejecutado en el presente proyecto en la Figura 9 se puede observar la ticketera con la información de alerta generada en la Figura 8.

Figura 9

Ticket generado en la plataforma de monitoreo de ciberseguridad



Fuente: SIEM de la empresa de Telecomunicaciones y ciberseguridad

Capítulo 5

5. Implementación de una plataforma SOAR

El presente capítulo se enfoca en la implementación de una plataforma SOAR para llevar a cabo el proceso automatizado de notificación y respuesta ante incidentes de accesos no autorizados a los sistemas críticos.

5.1. Diseño de diagramas de flujo del proceso de notificación y respuesta de alerta

En esta sección se muestran los diagramas de flujo del proceso de notificación y respuesta de alertas de autenticación sospechosas. En ellos se detalla, paso a paso, cómo se gestiona una alerta desde el momento en que es detectada hasta la respuesta automática, lo que permite comprender claramente la secuencia de acciones del proceso.

5.2. Implementación del flujo de proceso automatizado de notificación de alerta mediante SOAR

Esta sección se centra en convertir el diseño conceptual en una realidad funcional. Se usan las capacidades de la plataforma para notificar, de manera eficiente y precisa, sobre alertas de accesos no autorizados. En la Figura 10 se visualiza el flujo en SOAR para la notificación de la alerta al administrador del activo y en la Figura 11 se puede observar un ejemplo de la notificación mediante Telegram.

Figura 10

Automatización en SOAR del proceso de notificación de alerta

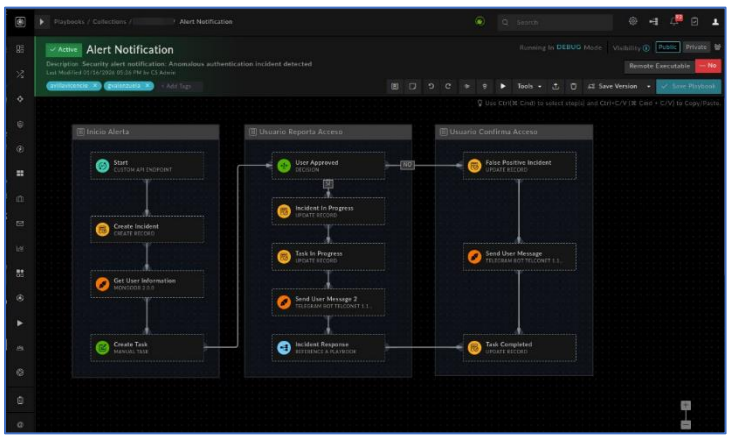


Figura 11

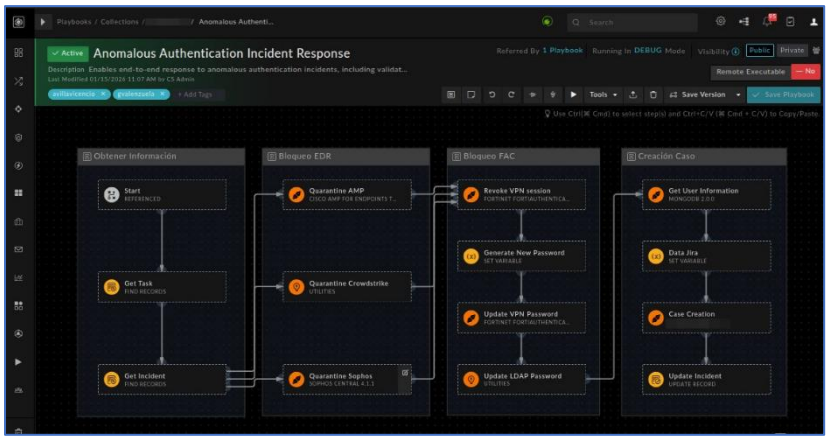
Notificación al administrador del activo vía Telegram de alerta presentada

5.3. Implementación del flujo de proceso automatizado de respuesta ante alerta mediante SOAR

Esta sección implementa el flujo de proceso automatizado de respuesta ante alerta mediante SOAR. Aquí, se detalla cómo la plataforma SOAR se utiliza para ejecutar respuestas predefinidas y medidas correctivas de manera automatizada ante incidentes de accesos no autorizados, mejorando así la eficacia y la rapidez en la mitigación de posibles riesgos, el flujo se observa en la Figura 12.

Figura 12

Automatización de respuesta del custodio vía telegram



5.4. Gobernanza operativa del flujo SOAR

El flujo de respuesta propuesto se ejecuta de forma automatizada mediante la plataforma SOAR. Sin embargo, para asegurar su correcta operación, se definió un esquema de gobernanza que establece responsabilidades, acuerdos de nivel de servicio (SLA) y controles de seguridad asociados al proceso de validación humana, en coherencia con los indicadores definidos en la metodología y evaluados durante el piloto controlado.

5.4.1. Matriz RACI del flujo SOAR

La Tabla 4 presenta la matriz RACI (R: Responsible – A: Accountable – C: Consulted – I: Informed) definida para las actividades que se vinculan con el flujo en SOAR para el sistema de alerta temprana y respuesta ante accesos administrativos anómalos.

Tabla 4

RACI del flujo de SOAR

Actividad	Equipo CSOC	Administrador de sistema
Detección y correlación de eventos	R/A	I
Generación automática de alerta	R/A	I
Notificación del evento	R/A	I
Confirmación del acceso	I	R/A
Escalamiento por no respuesta	R/A	I

Fuente: Matriz RACI sobre el flujo de notificación y respuesta ante accesos administrativos anómalos

Nota: El equipo CSOC agrupa las funciones de monitoreo, análisis y orquestación descritas en los capítulos previos, sin diferenciar niveles jerárquicos para efectos de este trabajo.

5.4.2. SLA de confirmación y escalamiento

Los acuerdos de nivel de servicio para el flujo SOAR se ajustan a los criterios de éxito de la metodología y a los resultados del piloto controlado.

- **Confirmación del responsable del sistema**: Tiempo objetivo ≤ 15 minutos desde la notificación del evento.
- **Escalamiento automático**: En caso de no recibir confirmación dentro del tiempo establecido, el SOAR escala automáticamente el evento para su gestión prioritaria por el equipo CSOC.
- **Gestión del incidente**: El tiempo máximo para la validación y gestión del evento corresponde a 120 minutos, en concordancia con el indicador TTR definido para alertas de severidad alta.

Estos SLA permiten estandarizar el proceso de respuesta y asegurar coherencia entre detección, validación y gestión del incidente.

5.4.3. Controles de seguridad del canal de mensajería

El canal de mensajería utilizado para la confirmación del evento es Telegram, con números corporativos para los involucrados en las diferentes actividades dentro del sistema.

- **Autenticación (Auth):** Las notificaciones son enviadas exclusivamente a la cuenta de Telegrama identificada por el ChatId (Identificador único) asociado número telefónico corporativo asignado al responsable del sistema, previamente registrado e inventariado por la organización.
- **Prevención de suplantación (Anti-impersonation):** El SOAR únicamente procesa respuestas provenientes los ChatId de Telegram registrados. Cualquier respuesta originada desde una cuenta distinta es descartada automáticamente.

El dispositivo asociado cuenta con agentes EDR y se encuentra bajo monitoreo del equipo de Seguridad Lógica.

- **Registro y trazabilidad:** Todas las interacciones asociadas al evento, incluyendo notificación, respuesta, tiempos de confirmación y estado final, quedan registradas en la plataforma SOAR y en la ticketera utilizada pro el equipo de monitoreo de ciberseguridad, garantizando auditoría y trazabilidad del flujo.

5.5. Evaluación de impacto

Basado en el piloto realizado se tienen indicadores resultantes presentado en la Tabla 5, los cuales concuerdan con los criterios de éxito definidos ex ante:

Tabla 5

Indicadores resultantes

Indicador	Antes	Después
MTTD (min)	90	15
TTR (min)	120	30
Falsos Positivos (%)	42	20
Eventos anómalos detectados (%)	50	85
SLA cumplidos (%)	70	95

Fuente: Mediciones realizadas por los autores en la ejecución piloto del sistema

Capítulo 6

6. Conclusiones y recomendaciones

6.1. Conclusiones

1. La implementación de un sistema de alerta temprana de autenticación permitió fortalecer el monitoreo sobre los accesos privilegiados a sistemas críticos, reduciendo significativamente el riesgo de accesos no autorizados en la infraestructura tecnológica evaluada.
2. La solución desarrollada demostró ser compatible con las herramientas ya existentes en la organización, evitando la necesidad de adquirir nuevos sistemas o realizar cambios en la arquitectura actual.
3. Las pruebas realizadas en un entorno controlado validaron la capacidad del sistema para generar alertas efectivas ante escenarios definidos como riesgo, permitiendo una respuesta rápida y oportuna por parte del personal responsable.
4. El uso de eventos de autenticación como insumo principal resultó ser una estrategia efectiva para identificar comportamientos anómalos sin afectar el rendimiento de los sistemas monitoreados.
5. La solución contribuye directamente a mejorar los controles del Sistema de Gestión de Seguridad de la Información (SGSI) al brindar visibilidad sobre actividades críticas, alineándose con lo establecido en la norma ISO/IEC 27002.

6.2. Recomendaciones

- Mantener actualizadas las reglas de correlación y umbrales definidos en el sistema de alertas, para asegurar su eficacia frente a la evolución de patrones de uso y amenazas emergentes.

- Incluir el monitoreo de nuevos sistemas o servicios críticos que se integren a la infraestructura tecnológica, para ampliar el alcance del sistema de alertas de forma progresiva.
- Incluir en el sistema la plataforma encargada del registro y autorización de los trabajos programados a fin de reducir los falsos positivos generados.
- Realizar revisiones periódicas de los registros de autenticación para identificar posibles puntos ciegos o fuentes de datos que no estén siendo consideradas actualmente.
- Capacitar al personal encargado de la administración de las alertas en el uso básico del sistema, a fin de garantizar una respuesta oportuna y una gestión adecuada de los eventos detectados.
- Evaluar la posibilidad de integrar las alertas generadas con plataformas de respuesta automática o flujos de escalamiento existentes, para optimizar la reacción ante incidentes sin aumentar la carga operativa.
- Ante nuevas tecnologías emergentes la arquitectura puede adaptarse al uso de inteligencia artificial por lo cual se recomienda integrar el sistema y los flujos enfocándolos hacia un nuevo estudio, mismo que pueda reducir la carga operativa del equipo de monitoreo como de los administradores de sistemas críticos.

Bibliografía

[1] A. Almehmadi y K. El-Khatib, «Authorized! Access Denied, Unauthorized! Access Granted», en Proceedings of the 6th International Conference on Security of Information and Networks, en SIN '13. New York, NY, USA: Association for Computing Machinery, 2013, pp. 363-367. doi: 10.1145/2523514.2523612.

[2] S. M. M. Hossain, R. Couturier, J. Rusk, y K. B. Kent, «Automatic Event Categorizer for SIEM», en Proceedings of the 31st Annual International Conference on Computer Science and Software Engineering, en CASCON '21. USA: IBM Corp., 2021, pp. 104-112.

[3] P. Wichmann, M. Marx, H. Federrath, y M. Fischer, «Detection of Brute-Force Attacks in End-to-End Encrypted Network Traffic», en Proceedings of the 16th International Conference on Availability, Reliability and Security, en ARES '21. New York, NY, USA: Association for Computing Machinery, 2021. doi: 10.1145/3465481.3470113.

[4] Asamblea Nacional, «Ley organica de protección de datos personales». 21 de mayo de 2021. [En línea]. Disponible en: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf Accedido: 21-ago-2025.

[5] W. U. Hassan, A. Bates, y D. Marino, «Tactical Provenance Analysis for Endpoint Detection and Response Systems», en 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 1172-1189. doi: 10.1109/SP40000.2020.00096.

[6] «IEEE Standard for Learning Technology–ECMAScript Application - Programming Interface for Content to Runtime Services Communication - Redline», IEEE Std 1484112-2020 Revis. IEEE Std 1148112-2003 - Redline, pp. 1-60, 2021.

[7] Asociación Española de Normalización, «UNE-EN ISO/IEC 27000», "Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Visión de conjunto y vocabulario," UNE, 15-dic-2021. [En línea]. Disponible: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0067945. Accedido: 20-oct-2025.

[8] "Modelo de Seguridad CIA," Ciberseguridad-Crimi CEU, 20-abr-2021. [En línea]. Disponible en: https://ciberseguridadcrimiceu.blogspot.com/2021/04/modelo-de-seguridad-cia.html. Accedido: 11-jul-2025.

[9] The International Organization for Standardization, «ISO/IEC 27032:2023(en)», ISO/IEC 27032:2023(en), Cybersecurity - Guidelines for Internet security. [En línea]. Disponible en: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27032:ed-2:v1:en Accedido: 18-oct-2025.

[10] Fortinet, «Fortinet», Líder global en soluciones y servicios de ciberseguridad | Fortinet. [En línea]. Disponible en: https://www.fortinet.com/lat Accedido: 20-oct-2025.

[11] Berkeley, «Berkeley», Berkeley Boot Camps. [En línea]. Disponible en: https://bootcamp.berkeley.edu/blog/what-is-computer-security/ Accedido: 20-oct-2025.

[12] kaspersky, «kaspersky», Soluciones de ciberseguridad de Kaspersky para hogares y empresas | Kaspersky. [En línea]. Disponible en: https://www.kaspersky.es/resource-center/definitions Accedido: 20-oct-2025.

[13] E. A. Lavrov, A. A. Volosiuk, N. B. Pasko, V. P. Gonchar, y G. K. Kozhevnikov, «Computer Simulation of Discrete Human-Machine Interaction for Providing Reliability and Cybersecurity of Critical Systems», en 2018 Third International Conference on Human Factors in Complex Technical Systems and Environments (ERGO)s and Environments (ERGO), 2018, pp. 67-70. doi: 10.1109/ERGO.2018.8443846.

[14] «PCI Security Standards Council», pcisecuritystandards. [En línea]. Disponible en: https://www.pcisecuritystandards.org/glossary/critical-systems-critical-technologies/. Accedido: 20-oct-2025.