SISTEMATIZACIÓN DEL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA MEDIANTE CONTROLES DE CIBERSEGURIDAD Y GESTIÓN DE IDENTIDADES EN COLSUBSIDIO

JULIÁN ESTEBAN GAMBOA PRIETO

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C.
2026

SISTEMATIZACIÓN DEL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA MEDIANTE CONTROLES DE CIBERSEGURIDAD Y GESTIÓN DE IDENTIDADES EN COLSUBSIDIO

JULIÁN ESTEBAN GAMBOA PRIETO
TUTOR: RAFAEL ORLANDO CUBILLOS SANCHEZ

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C.
2026

Tabla de contenido

RESUMEN

La presente monografía sistematiza el fortalecimiento de la seguridad informática en Colsubsidio a partir de los controles de ciberseguridad y la gestión de identidades implementados en la Gerencia de Tecnología, área de Seguridad Informática, durante el periodo de práctica comprendido entre el 15 de julio de 2025 y el 14 de enero de 2026. El estudio se enmarca en un enfoque descriptivo tipo estudio de caso y se apoya en la revisión de evidencias generadas por herramientas especializadas como Azure Entra ID, Qualys, CrowdStrike y SAP, así como en matrices de acceso, inventarios de conectividad y reportes para revisoría fiscal.

En el componente de ciberseguridad se analizan los controles de monitoreo de identidades en la nube mediante autenticación multifactor y acceso condicional, la gestión de vulnerabilidades en veinticuatro portales web y la respuesta ante alertas de seguridad en endpoints, junto con la verificación periódica de direcciones IP en listas negras para preservar la disponibilidad y reputación de los servicios tecnológicos. En el componente de gestión de identidades se estudian los procesos de revisión de usuarios no genéricos, la depuración de más de mil roles obsoletos en SAP y el control mensual de ciento trece transacciones críticas, orientados a reforzar el principio de mínimo privilegio y la segregación de funciones en los sistemas ERP y aplicativos asociados.

Los resultados evidencian una mejora en la trazabilidad de accesos privilegiados, una mayor visibilidad sobre vulnerabilidades y una consolidación de las evidencias requeridas por auditoría interna y revisoría fiscal, demostrando que la articulación entre IAM, gestión de vulnerabilidades y seguridad de red constituye un pilar fundamental para la protección de los activos tecnológicos de la organización. Asimismo, la sistematización de esta experiencia aporta un marco de referencia práctico para la implementación y seguimiento de controles de seguridad de la información en entornos corporativos complejos.

Palabras clave

Seguridad de la información; ciberseguridad; gestión de identidades y accesos (IAM); autenticación multifactor (MFA); gestión de vulnerabilidades; ERP; SAP; listas negras de IP; filtrado web; controles de acceso, Azure Entra ID, Qualys, CrowdStrike, endpoints, portales web.

1. INTRODUCCIÓN

Las pasantías profesionales constituyen una etapa fundamental en la formación académica, ya que permiten aplicar de manera práctica los conocimientos adquiridos durante el proceso educativo, fortalecer competencias técnicas y desarrollar habilidades profesionales en entornos reales de trabajo. En el ámbito de la tecnología y la seguridad de la información, esta experiencia resulta especialmente relevante debido al crecimiento de las amenazas cibernéticas y a la necesidad de que las organizaciones implementen controles robustos para proteger sus activos digitales, la información y los sistemas críticos.

En este contexto, las pasantías se desarrollaron en Colsubsidio, una de las cajas de compensación familiar más importantes del país, dentro de la Gerencia de Tecnología, específicamente en la Subdirección Organizacional, en el área de Seguridad Informática, enfocada en Ciberseguridad y Gestión de Identidades. El periodo de prácticas se extendió entre el 15 de julio de 2025 y el 14 de enero de 2026, durante el cual el practicante se integró a un entorno organizacional con altos estándares en la gestión de la seguridad de la información.

Durante la experiencia de pasantías, el trabajo realizado se orientó al fortalecimiento de los controles de seguridad y a la correcta administración de identidades y accesos dentro de la organización, contribuyendo al cumplimiento de políticas internas, lineamientos normativos y buenas prácticas en seguridad de la información. Esta participación permitió evidenciar la importancia de los procesos de monitoreo, control y auditoría como pilares fundamentales para la protección de los sistemas de información en una entidad de gran tamaño y complejidad tecnológica.

El presente documento tiene como finalidad exponer de manera ordenada y analítica el desarrollo de las pasantías, evidenciando el impacto de esta experiencia en la formación profesional y la aplicación de los conocimientos teóricos en un contexto real. Asimismo, se busca resaltar los aportes realizados al área de Seguridad Informática de Colsubsidio y los aprendizajes adquiridos a nivel técnico, metodológico y ético, los cuales fortalecen el perfil profesional del practicante y aportan valor a su proceso académico y laboral futuro.

2. COLSUBSIDIO

Colsubsidio, es una corporación privada sin ánimo de lucro fundada el 19 de septiembre de 1957 en Bogotá, integrada al Sistema de Subsidio Familiar y al Sistema de Seguridad Social de Colombia. La empresa fue creada por iniciativa de la Asociación Nacional de Industriales (ANDI) con el propósito de otorgar subsidios y prestaciones sociales a trabajadores afiliados, ampliando posteriormente su portafolio de servicios.

Propósito y Misión: La organización ha definido su propósito superior como "Generar oportunidades para el cierre de brechas sociales", trabajando día a día para mejorar la calidad de vida de sus afiliados y sus familias mediante la entrega de subsidios y servicios integrales. Con más de 65 años de trayectoria, Colsubsidio se posiciona como la empresa social líder en Colombia, reconocida por su capacidad de anticipación y apertura al cambio, lo que le ha permitido adaptarse a las dinámicas cambiantes del país y responder a las expectativas de sus empresas, trabajadores y comunidades.

Colsubsidio cuenta con una cobertura nacional y representa un actor significativo en la economía social colombiana:

- 1.4 a 1.6 millones de trabajadores afiliados que disfrutan de sus servicios
- Más de 95,000 empresas afiliadas que utilizan sus programas
- Presencia a nivel nacional en Colombia
- Posicionamiento como empresa número 1 en innovación según ANDI
- Reconocimiento como 9.° empleador más grande del país
- Primera caja de compensación en número de afiliados

En términos de desempeño financiero y empresarial, Colsubsidio figura entre las principales empresas colombianas, ubicándose en el número 23 en ingresos, número 28 en responsabilidad corporativa, número 39 en reputación corporativa y número 31 en capacidad para atraer y retener talento.

Estructura Organizacional: Colsubsidio opera bajo una estructura corporativa tradicional compuesta por:

- Asamblea General: Órgano máximo de gobierno que elige al Consejo Directivo, designa revisor fiscal y aprueba cuentas y estados financieros.

- Consejo Directivo: Responsable de la suprema dirección administrativa, adopta políticas administrativas y financieras.
- Dirección Administrativa: Dirigida por el Director Administrativo, encargada de la ejecución operativa (Luis Carlos Arango Velez).
- Subdirecciones: Incluyen Gestión Organizacional, Financiera, Salud y otras especialidades.
- Gerencias especializadas: Entre ellas, Tecnología.

La Gerencia de Tecnología bajo la Subdirección de Gestión Organizacional es responsable de diseñar, sustentar y monitorear estrategias que aseguren la continuidad operativa mediante sistemas, procesos de TI, tecnologías y plataformas que soporten el crecimiento, competitividad y transformación digital de Colsubsidio. Dentro de esta gerencia opera el Área de Seguridad Informática, que se subdivide en dos componentes estratégicos:

1. Ciberseguridad: Protección contra amenazas externas e internas, monitoreo de infraestructura
2. Gestión de Identidades: Control de accesos, administración de permisos y cumplimiento normativo

3. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, las organizaciones dependen cada vez más de las tecnologías de la información para gestionar sus procesos operativos, administrativos y estratégicos. La transformación digital ha permitido mejorar la eficiencia en el manejo de datos, la automatización de procesos y la conectividad entre diferentes áreas de una empresa. Sin embargo, esta creciente dependencia tecnológica también ha generado nuevos desafíos relacionados con la protección de la información, el control de accesos a los sistemas y la gestión de vulnerabilidades en las infraestructuras tecnológicas.

Uno de los principales retos que enfrentan las organizaciones modernas es garantizar la seguridad de sus sistemas de información frente a amenazas internas y externas. Los ciberataques, el uso indebido de credenciales, las configuraciones incorrectas en plataformas tecnológicas y las vulnerabilidades en aplicaciones empresariales representan riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. Estas situaciones pueden generar pérdidas económicas, afectaciones operativas e impactos negativos en la reputación de la organización.

En este contexto, las áreas de ciberseguridad dentro de las empresas desempeñan un papel fundamental en la implementación de estrategias orientadas a fortalecer la protección de los sistemas tecnológicos. Estas estrategias incluyen la gestión adecuada de identidades digitales, el control de accesos a plataformas empresariales, el monitoreo de vulnerabilidades en los sistemas y la implementación de herramientas tecnológicas especializadas que permitan identificar y mitigar posibles amenazas.

No obstante, la correcta implementación de estos controles requiere no solo el uso de herramientas tecnológicas avanzadas, sino también la participación de profesionales capacitados que contribuyan a la gestión y análisis de la seguridad informática dentro de la organización. En este sentido, las prácticas profesionales representan una oportunidad para que los estudiantes participen activamente en procesos reales de ciberseguridad, aplicando los conocimientos adquiridos durante su formación académica en un entorno laboral.

A partir de lo anterior, surge la necesidad de analizar cómo el desarrollo de actividades relacionadas con la gestión de accesos, el monitoreo de vulnerabilidades y el uso de herramientas de seguridad informática contribuye al

fortalecimiento de la protección de los sistemas empresariales. En este contexto, la presente monografía busca documentar y analizar las actividades realizadas durante el periodo de práctica profesional en el área de ciberseguridad, describiendo los procesos, herramientas y aprendizajes obtenidos durante esta experiencia.

4. JUSTIFICACIÓN

En el contexto actual de transformación digital, las organizaciones dependen cada vez más de sistemas tecnológicos para gestionar sus procesos operativos, administrativos y estratégicos. El uso de plataformas digitales, sistemas empresariales, servicios en la nube y herramientas tecnológicas ha permitido mejorar la eficiencia en el manejo de la información y optimizar los procesos internos. Sin embargo, este crecimiento tecnológico también ha incrementado los riesgos asociados a la seguridad de la información, generando la necesidad de implementar mecanismos de protección que garanticen la confidencialidad, integridad y disponibilidad de los datos.

En este escenario, la ciberseguridad se ha convertido en un elemento fundamental dentro de las estrategias organizacionales, ya que permite proteger los sistemas informáticos frente a amenazas como ataques cibernéticos, accesos no autorizados, robo de información y explotación de vulnerabilidades en las infraestructuras tecnológicas. Las organizaciones deben implementar controles de seguridad adecuados que permitan prevenir incidentes de seguridad y garantizar la continuidad de sus operaciones.

Uno de los aspectos más relevantes dentro de la seguridad informática es la gestión adecuada de identidades y accesos a los sistemas tecnológicos. En entornos empresariales donde múltiples usuarios interactúan con diferentes plataformas, resulta fundamental establecer mecanismos que permitan controlar quién puede acceder a determinados recursos y en qué condiciones. Una gestión inadecuada de accesos puede generar riesgos significativos, como el uso indebido de credenciales, accesos no autorizados o la exposición de información sensible.

De igual manera, la identificación y gestión de vulnerabilidades en los sistemas tecnológicos representa un proceso clave para fortalecer la seguridad de la infraestructura informática. Las vulnerabilidades pueden presentarse en aplicaciones, sistemas operativos, redes o configuraciones de seguridad, y si no son identificadas oportunamente pueden ser aprovechadas por actores maliciosos para comprometer los sistemas de una organización. Por esta razón, las empresas implementan herramientas especializadas que permiten detectar debilidades en los sistemas y aplicar medidas correctivas para mitigar los riesgos asociados.

En este contexto, el desarrollo de prácticas profesionales en el área de ciberseguridad adquiere una gran importancia dentro de la formación académica de

los estudiantes de programas relacionados con tecnologías de la información. Las pasantías permiten que los estudiantes tengan la oportunidad de aplicar los conocimientos adquiridos durante su proceso formativo en un entorno laboral real, participando en actividades relacionadas con la gestión de seguridad informática, el análisis de sistemas y el uso de herramientas tecnológicas especializadas.

La presente monografía se justifica en la necesidad de documentar y analizar la experiencia adquirida durante el desarrollo de la práctica profesional en el área de ciberseguridad de una organización. A través de este documento se busca describir las actividades realizadas, las herramientas utilizadas y los conocimientos aplicados durante el periodo de pasantía, evidenciando la relación entre la formación académica y la práctica profesional en el ámbito de la seguridad informática.

Asimismo, este trabajo permite evidenciar la importancia de la ciberseguridad dentro de las organizaciones modernas y cómo la implementación de controles adecuados contribuye a la protección de los sistemas tecnológicos y la información empresarial. El análisis de las actividades desarrolladas durante la práctica profesional permite comprender la relevancia de la gestión de accesos, el monitoreo de vulnerabilidades y el uso de herramientas de seguridad como elementos clave dentro de las estrategias de protección de la infraestructura tecnológica.

Finalmente, esta monografía también representa un aporte académico al documentar una experiencia práctica dentro del área de ciberseguridad, permitiendo evidenciar el impacto que tiene la participación de los estudiantes en procesos reales dentro de una organización. De esta manera, se fortalece la relación entre el conocimiento teórico adquirido en la universidad y su aplicación en contextos laborales, contribuyendo al desarrollo de profesionales con competencias técnicas y analíticas orientadas a la protección de la información y la seguridad de los sistemas tecnológicos.

5. OBJETIVOS

5.1 Objetivo General

Sistematizar el fortalecimiento de la seguridad informática en Colsubsidio mediante el análisis de los controles de ciberseguridad y gestión de identidades implementados en la Gerencia de Tecnología.

5.2 Objetivos Específicos

- Analizar el estado de las identidades en la nube y el uso de autenticación multifactor (MFA) en Azure Entra ID para identificar cuentas y accesos con riesgos.

- Identificar y clasificar vulnerabilidades en veinticuatro portales web mediante escaneos con Qualys y alertas de CrowdStrike para priorizar su mitigación.

- Optimizar los permisos en los sistemas SAP mediante la revisión de usuarios, la eliminación de roles obsoletos y el control de transacciones críticas.

- Verificar la reputación de la infraestructura de red y de los accesos privilegiados mediante la revisión de IP en listas negras y la generación de evidencias para revisoría fiscal.

6. MARCO TEÓRICO

6.1 Fundamentos de Seguridad de la Información

En la actualidad, las organizaciones dependen en gran medida de infraestructuras tecnológicas para el almacenamiento, procesamiento y transmisión de información crítica. Esta dependencia ha incrementado la necesidad de implementar mecanismos robustos de seguridad que permitan proteger los activos digitales frente a amenazas internas y externas. La seguridad de la información se define como el conjunto de políticas, procedimientos y tecnologías orientadas a proteger la información y los sistemas que la gestionan contra accesos no autorizados, alteraciones o interrupciones del servicio [8].

Uno de los principios fundamentales de la seguridad de la información es la tríada de seguridad, conocida también como modelo CIA (Confidentiality, Integrity, Availability). Este modelo establece tres pilares esenciales para la protección de la información dentro de cualquier sistema tecnológico [45].

- La confidencialidad se refiere a la protección de la información contra accesos no autorizados. Este principio garantiza que únicamente las personas o sistemas autorizados puedan acceder a datos sensibles. Para lograrlo, las organizaciones implementan mecanismos como autenticación, control de accesos, cifrado de datos y políticas de seguridad [45].

- La integridad hace referencia a la precisión y consistencia de los datos durante todo su ciclo de vida. Esto significa que la información no debe ser alterada de manera indebida, ya sea de forma accidental o maliciosa. Para preservar la integridad de los datos se utilizan controles como firmas digitales, registros de auditoría y mecanismos de validación de información [6] [45].

- Por otra parte, la disponibilidad garantiza que la información y los sistemas estén accesibles cuando los usuarios autorizados los requieran. Este principio implica la implementación de medidas que aseguren la continuidad del servicio, tales como sistemas de respaldo, redundancia de infraestructura y planes de recuperación ante desastres [48] [12].

En la práctica, la implementación de la tríada CIA implica balancear prioridades: elevar al máximo la confidencialidad puede afectar disponibilidad o usabilidad,

mientras que priorizar solo disponibilidad puede debilitar los mecanismos de control de acceso. Por ello, las organizaciones definen políticas y niveles de servicio alineados con el apetito de riesgo, la criticidad de los procesos y los requisitos regulatorios [43] [45].

Además de la tríada de seguridad, otro elemento clave dentro de la gestión de seguridad es la gestión de riesgos. Este proceso consiste en identificar, analizar y mitigar los riesgos que pueden afectar los activos tecnológicos de una organización. La gestión de riesgos permite priorizar amenazas y vulnerabilidades según su impacto y probabilidad de ocurrencia, facilitando la implementación de controles de seguridad adecuados [8].

Las normas internacionales, como la ISO/IEC 27001, establecen un marco de referencia para la implementación de sistemas de gestión de seguridad de la información. Estas normas proporcionan lineamientos para la identificación de riesgos, la implementación de controles y la mejora continua de la seguridad dentro de las organizaciones. En consecuencia, la seguridad de la información se convierte en un elemento estratégico dentro de las organizaciones modernas, ya que permite proteger la información crítica, garantizar la continuidad operativa y cumplir con requisitos regulatorios y normativos [43] [18].

6.2 Gestión de identidades y accesos (IAM)

La gestión de identidades y accesos (Identity and Access Management, IAM) se define como el conjunto de políticas, procesos y tecnologías que permiten administrar el ciclo de vida completo de las identidades digitales y controlar su acceso a los recursos de la organización, tanto en entornos on-premise como en la nube. IAM es hoy un control fundamental de la seguridad en la nube y un habilitador de modelos como trabajo remoto y arquitecturas de confianza cero [8].

Concepto y objetivos de IAM

Un sistema IAM asigna a cada usuario, dispositivo o servicio una identidad digital única asociada a atributos, roles y privilegios, que determinan qué recursos puede usar y en qué condiciones. El objetivo central es garantizar que cada identidad tenga únicamente los permisos necesarios para desempeñar sus funciones, minimizando el riesgo de accesos indebidos, fraudes internos o incumplimientos normativos [18].

Entre los componentes típicos de una solución IAM se encuentran:

- Repositorio de identidades: base de datos o directorio donde se almacenan cuentas, atributos y estados de usuarios (altas, bajas, cambios, bloqueo, expiración).

- Mecanismos de autenticación: procesos que verifican que quien intenta acceder corresponde realmente a la identidad declarada (contraseñas, MFA, certificados, biometría).

- Mecanismos de autorización: reglas que determinan a qué recursos puede acceder cada identidad y con qué nivel de privilegio, frecuentemente mediante modelos de control de acceso basado en roles (RBAC) o basado en atributos (ABAC).

- Gobernanza de identidades: procesos para revisar periódicamente accesos, detectar cuentas huérfanas o privilegios excesivos y asegurar el cumplimiento de políticas internas y marcos regulatorios.

En entornos cloud, los servicios de directorio como Azure Entra ID permiten centralizar identidades para aplicaciones locales y en la nube, facilitar el inicio de sesión único (SSO) y aplicar políticas de acceso condicional en función de factores como ubicación, tipo de dispositivo o estado de la cuenta [3] [4].

Ciclo de vida de la identidad digital

La buena gestión de identidades implica considerar el ciclo de vida completo del usuario, desde su incorporación hasta su salida de la organización [18].

1. Aprovisionamiento: creación de la identidad y asignación inicial de roles y permisos, basada generalmente en el cargo, unidad organizacional y funciones a desempeñar.

2. Cambios: ajustes por traslados, ascensos, cambios de rol o necesidades temporales; deben gestionarse con criterios de mínima exposición temporal y registro de aprobaciones.

3. Desaprovisionamiento: desactivación o eliminación oportuna de cuentas cuando un colaborador se retira o cambia de rol, reduciendo el riesgo de cuentas huérfanas que puedan ser explotadas.

Automatizar este ciclo, integrando IAM con sistemas de recursos humanos o directorios corporativos, reduce errores manuales y mejora la trazabilidad [18] [8].

Autenticación multifactor (MFA) y acceso condicional

La autenticación multifactor (MFA) es una tecnología que exige al usuario presentar dos o más factores de verificación independientes para validar su identidad antes de acceder a un sistema o servicio. Estos factores suelen agruparse en [10]:

- Algo que el usuario sabe: contraseñas o PIN [10].
- Algo que el usuario tiene: tokens físicos, aplicaciones generadoras de códigos, tarjetas inteligentes [10].
- Algo que el usuario es: rasgos biométricos como huella digital o reconocimiento facial [10].

La MFA reduce de forma significativa el riesgo asociado al robo de credenciales, ya que comprometer una contraseña por sí sola no basta para acceder a los sistemas protegidos. En entornos cloud, suele complementarse con políticas de acceso condicional, que modifican los requisitos de autenticación en función de parámetros como ubicación geográfica, reputación de la IP, tipo de dispositivo o criticidad de la aplicación [4] [18].

Principio de mínimo privilegio y segregación de funciones

El principio de mínimo privilegio establece que cada usuario debe contar únicamente con los permisos imprescindibles para realizar sus tareas, durante el tiempo estrictamente necesario. Aplicar este principio reduce la superficie de ataque frente a amenazas internas y limita el daño potencial causado por credenciales comprometidas [52].

En paralelo, la segregación de funciones (SoD, Segregation of Duties) busca evitar que una misma persona concentre actividades incompatibles que puedan dar lugar a fraudes o errores graves, por ejemplo, crear proveedores y aprobar pagos en un sistema financiero. Para lograrlo se diseñan matrices de acceso que identifican combinaciones de roles o transacciones consideradas riesgosas y se configuran controles preventivos y detectivos para impedir su acumulación [49].

Las plataformas IAM y los módulos de gobierno de accesos en ERP permiten automatizar análisis de SoD, generar alertas por conflictos de funciones y documentar las justificaciones y aprobaciones necesarias cuando ciertas combinaciones son inevitables [2].

6.3 Gestión de vulnerabilidades y respuesta ante amenazas

La gestión de vulnerabilidades y la respuesta ante amenazas constituyen otro eje central de la ciberseguridad corporativa, complementando a IAM y al control de accesos. Mientras IAM se centra en quién accede y con qué permisos, la gestión de vulnerabilidades se enfoca en las debilidades técnicas de sistemas, aplicaciones y redes, y la respuesta ante amenazas se orienta a la detección y contención de actividades maliciosas en tiempo real [18] [51].

Concepto de vulnerabilidad y su ciclo de gestión

Una vulnerabilidad es una debilidad en software, hardware, procesos o configuraciones que puede ser explotada por una amenaza para comprometer un activo. El ciclo típico de gestión de vulnerabilidades incluye [12]:

1. Descubrimiento: identificación de activos y escaneo de vulnerabilidades mediante herramientas automáticas.

2. Evaluación: análisis de severidad y priorización según el impacto potencial sobre confidencialidad, integridad y disponibilidad.

3. Tratamiento: aplicación de parches, cambios de configuración, segmentación o medidas compensatorias.

4. Verificación: reescaneos y pruebas que confirman la remediación.

Las plataformas de escaneo automatizado permiten identificar de forma periódica fallas de configuración, versiones desactualizadas o errores en aplicaciones web, generando reportes que se integran a los procesos de gestión de cambios y de riesgos [13].

Common Vulnerability Scoring System (CVSS)

El Common Vulnerability Scoring System (CVSS) es un estándar internacional para medir la gravedad de las vulnerabilidades de seguridad en software y sistemas, mediante una escala numérica de 0,0 a 10,0 que se traduce en rangos cualitativos desde bajo hasta crítico. CVSS está gestionado por el Forum of Incident Response and Security Teams (FIRST) y se ha convertido en referencia para priorizar esfuerzos de remediación [50].

Las métricas de CVSS se agrupan en tres grandes bloques:

- Métricas base: describen las características intrínsecas de una vulnerabilidad que no cambian con el tiempo ni según el entorno (vector de ataque, complejidad, privilegios requeridos, interacción del usuario, impacto sobre confidencialidad, integridad y disponibilidad) [50].

- Métricas temporales o de amenaza: reflejan factores que evolucionan, como la existencia de código de explotación público o la disponibilidad de parches [50].

- Métricas ambientales: adaptan la puntuación al contexto particular de una organización, considerando la criticidad de los activos afectados y requisitos específicos [50].

Al incorporar CVSS en los flujos de trabajo de escaneo de vulnerabilidades, las organizaciones pueden comparar fallas entre distintos sistemas, priorizar correcciones y comunicar el riesgo de forma estandarizada a equipos técnicos y de negocio [50].

Análisis de vulnerabilidades en aplicaciones web

Las aplicaciones web son un vector frecuente de ataque debido a su exposición directa a internet y a la complejidad de sus componentes. El análisis de vulnerabilidades web se apoya en herramientas que ejecutan escaneos automáticos sobre los portales, identificando debilidades como inyecciones de código, exposiciones de información sensible, configuraciones inseguras o uso de bibliotecas desactualizadas.

Los resultados se clasifican según su severidad, normalmente vinculados a puntuaciones CVSS, y se acompañan de recomendaciones de remediación. En el contexto de una organización que administra decenas de portales corporativos, como ocurre en muchas entidades de servicios, estos escaneos periódicos constituyen un insumo crítico para la mejora continua de la postura de seguridad [39] [49].

Endpoint Detection and Response (EDR)

La detección y respuesta para endpoints (Endpoint Detection and Response, EDR) es una categoría de soluciones que combinan monitoreo continuo de endpoints, recolección de datos de actividad, análisis avanzado y capacidad de respuesta automatizada frente a amenazas. Los endpoints incluyen estaciones de trabajo, servidores, dispositivos móviles y otros equipos conectados a la red corporativa [18] [19].

Las principales funciones de un sistema EDR son:

- Monitoreo y registro de eventos en endpoints: procesos, conexiones de red, cambios en archivos, actividad de usuarios, entre otros.

- Análisis y correlación de estos eventos para identificar patrones sospechosos o indicadores de compromiso.

- Respuesta automatizada frente a actividades maliciosas, como el aislamiento del endpoint, la detención de procesos o el bloqueo de conexiones.

- Soporte a la investigación forense mediante historiales detallados de actividad, que permiten reconstruir la cadena de eventos de un incidente.

La adopción de EDR se ha incrementado por el aumento de la sofisticación de los ataques y la ampliación de la superficie de ataque, impulsada por el crecimiento de dispositivos conectados y modelos de trabajo remoto. Integrar EDR con otras capacidades, como los sistemas de correlación de eventos (SIEM) y las plataformas de orquestación y respuesta (SOAR), potencia la capacidad de detección temprana y respuesta coordinada ante incidentes [18] [19].

6.4 Seguridad en sistemas ERP y en SAP

Los sistemas de planificación de recursos empresariales (ERP) son plataformas integrales que centralizan procesos clave de la organización, como finanzas, compras, logística, recursos humanos y producción. Debido a la sensibilidad de la información que manejan y a su rol como núcleo transaccional, la seguridad en los ERP es crítica para asegurar la continuidad del negocio y el cumplimiento regulatorio [25] [24].

Concepto general de seguridad en ERP

La seguridad en ERP se enfoca en proteger la integridad, confidencialidad y disponibilidad de la información que gestiona el sistema, así como en garantizar que solo usuarios autorizados accedan a datos y funciones en línea con sus responsabilidades. Entre los aspectos clave destacan [25]:

- Control de acceso a nivel de módulos, transacciones y datos.
- Trazabilidad de acciones de los usuarios mediante registros de auditoría.
- Configuraciones de red y de infraestructura que protejan el servidor ERP frente a accesos no autorizados.
- Mecanismos de respaldo y recuperación para reducir el impacto de fallos técnicos o incidentes.

Dado que el ERP integra procesos financieros y operativos, cualquier brecha de seguridad puede tener consecuencias significativas, desde fraudes y pérdidas económicas hasta sanciones regulatorias por exposición de datos personales o fiscales [25].

Modelo de roles y autorizaciones en SAP

SAP es uno de los ERP más extendidos a nivel empresarial y cuenta con un modelo de seguridad basado en roles, perfiles y objetos de autorización [52]. En este modelo:

- Un rol agrupa un conjunto de transacciones, informes y autorizaciones necesarias para desempeñar un conjunto de funciones.

- Los objetos de autorización representan la unidad mínima de control y definen qué operaciones se permiten sobre determinados campos (por ejemplo, sociedades, centros, clases de documento).

- Los perfiles almacenan los datos de autorización generados a partir de los roles y se asignan a los usuarios.

El diseño adecuado de roles pasa por analizar las tareas reales de los usuarios, agruparlos según funciones comunes y crear roles específicos que otorguen únicamente los permisos indispensables, facilitando la segregación de funciones y reduciendo el riesgo de accesos innecesarios. Herramientas de gobierno de accesos, como SAP GRC o soluciones especializadas de terceros, permiten automatizar la detección de conflictos de SoD, gestionar solicitudes y aprobaciones de roles, y mantener la trazabilidad de cambios [52].

Riesgos por roles obsoletos y privilegios elevados

En entornos con larga historia de uso de SAP es frecuente que se acumulen roles obsoletos, usuarios inactivos con privilegios elevados o combinaciones de autorizaciones que ya no responden a la estructura organizacional actual. Estos escenarios incrementan la superficie de ataque y pueden generar hallazgos recurrentes en auditorías [52] [53].

Roles genéricos con acceso amplio, perfiles globales como SAP_ALL o SAP_NEW y autorizaciones no justificadas sobre transacciones críticas son ejemplos de configuraciones que vulneran el principio de mínimo privilegio. Las buenas prácticas recomiendan [53]:

- Depurar periódicamente roles no utilizados o que concentran privilegios excesivos.
- Revisar usuarios con accesos de alto riesgo y documentar justificaciones.
- Implementar controles periódicos sobre transacciones clasificadas como críticas por el negocio.

Estas actividades se alinean con las exigencias de revisores fiscales y auditores internos, que buscan evidencias objetivas de control sobre los accesos en el ERP [52] [53].

6.5 Seguridad de red, perímetro y reputación de IP

La seguridad de red y perímetro comprende los mecanismos que protegen la infraestructura de comunicaciones, controlan el tráfico entre redes internas y externas, y aplican políticas de filtrado de contenido y acceso a internet. En este ámbito, cobran relevancia tanto los firewalls de nueva generación como los servicios de reputación de direcciones IP y las listas negras [43] [40] [31].

Firewalls de nueva generación y filtrado web

Los firewalls de nueva generación no solo inspeccionan puertos y direcciones, sino también aplicaciones, contenidos y usuarios, permitiendo políticas más granulares de acceso. Una de sus funciones clave es el filtrado web, que bloquea o permite el acceso a sitios según categorías de contenido o listas definidas por la organización [26] [28].

Servicios como el filtrado web de FortiGuard clasifican millones de sitios en categorías (por ejemplo, riesgos de seguridad, contenido adulto, redes sociales, consumo de ancho de banda) basadas en su idoneidad para entornos empresariales, educativos o familiares. Las políticas corporativas suelen bloquear de forma predeterminada categorías consideradas de alto riesgo, como malware, phishing o contenido ilícito, y restringir aquellas que afectan productividad o ancho de banda [28].

La combinación de filtrado por categorías dinámicas y listas blancas/negras estáticas permite adaptar el control de navegación a las necesidades particulares de cada organización. Además, el registro de URL consultadas y decisiones de bloqueo sirve como evidencia ante incidentes o auditorías [28].

Reputación de direcciones IP y listas negras

La reputación de una dirección IP se refiere a la percepción que otros sistemas tienen sobre la confiabilidad del tráfico que se origina en ella, basada en el historial de envío de correo, comportamiento de red y reportes de abuso. Cuando una IP está asociada a envío de spam, malware o actividades maliciosas, puede ser incluida en listas negras (blacklists) mantenidas por comunidades especializadas o proveedores de servicios de internet [26].

Estar en una lista negra puede provocar que los correos de la organización sean bloqueados por filtros antispam, que ciertas conexiones se rechacen o que servicios críticos se vean interrumpidos, afectando la disponibilidad percibida por usuarios y clientes. Por ello, muchas organizaciones utilizan herramientas de verificación periódica de reputación de IP para detectar inclusiones en listas negras y gestionar solicitudes de retiro ante los proveedores o administradores de dichas listas.

Desde la perspectiva de la seguridad de la información, la reputación de IP se vincula con la confidencialidad y disponibilidad: una IP comprometida puede ser utilizada para distribuir código malicioso, mientras que su bloqueo indiscriminado puede interrumpir servicios legítimos [26] [34].

6.6 Articulación entre IAM, gestión de vulnerabilidades y seguridad de red

Aunque la gestión de identidades, la gestión de vulnerabilidades y la seguridad de red se abordan a menudo como dominios separados, en la práctica conforman un sistema interdependiente que soporta la seguridad integral de la organización [47].

- IAM controla quién accede a qué recursos y en qué condiciones, mediante identidades, autenticación y autorización.

- La gestión de vulnerabilidades y las plataformas de escaneo se centran en qué tan robustos son los sistemas y aplicaciones frente a las amenazas conocidas.

- La seguridad de red y las soluciones EDR se encargan de cómo se comporta el tráfico y la actividad en los endpoints y la infraestructura, detectando y respondiendo a anomalías.

El fortalecimiento de la seguridad informática requiere coordinar estos ámbitos: por ejemplo, la desactivación de cuentas y la depuración de roles en un ERP deben acompañarse de reglas de firewall y monitoreo que impidan accesos residuales desde direcciones IP sospechosas; de igual forma, los hallazgos de vulnerabilidades web deben traducirse en requisitos de autenticación y autorización más estrictos cuando se trate de portales con información sensible [47].

En organizaciones que operan múltiples herramientas especializadas directorios en la nube, escáneres de vulnerabilidades, plataformas EDR, firewalls de filtrado por categorías y sistemas ERP, el desafío teórico y práctico consiste en diseñar una

arquitectura de controles coherente, basada en modelos como la tríada CIA, el principio de mínimo privilegio, la segregación de funciones y la gestión de riesgos, que permita sistematizar la protección de los activos tecnológicos [54] [47].

7. METODOLOGÍA

La metodología empleada en este trabajo de grado corresponde a un estudio de caso de carácter descriptivo, orientado a sistematizar las actividades de fortalecimiento de la seguridad informática desarrolladas en Colsubsidio en los frentes de ciberseguridad y gestión de identidades durante el periodo de práctica profesional comprendido entre el 15 de julio de 2025 y el 14 de enero de 2026. El estudio se centra en documentar, organizar y analizar los controles implementados en la Gerencia de Tecnología, área de Seguridad Informática, con el fin de evidenciar su aporte a la protección de los activos tecnológicos y al cumplimiento de los lineamientos de seguridad de la información de la organización.

Desde el punto de vista del enfoque, la investigación es predominantemente cualitativa, ya que se basa en la descripción y análisis de procesos, controles y evidencias generadas en el contexto real de la operación de Colsubsidio; sin embargo, integra elementos cuantitativos simples, como el número de usuarios monitoreados, la cantidad de roles eliminados en SAP, el total de transacciones críticas controladas o el volumen de vulnerabilidades identificadas en los portales web. Esta combinación permite articular la comprensión de los procedimientos técnicos con indicadores básicos que apoyan la valoración de los resultados.

Diseño metodológico

El diseño metodológico se estructura como un estudio de caso único, en el que la unidad de análisis corresponde a los procesos y controles de seguridad de la información gestionados por el área de Seguridad Informática de Colsubsidio, específicamente en los componentes de ciberseguridad, gestión de identidades, seguridad en sistemas ERP y seguridad de red. A partir de esta unidad se organizan las actividades y evidencias en función de los objetivos específicos del trabajo: monitoreo de identidades en la nube, gestión de vulnerabilidades y alertas, optimización de permisos en SAP y verificación de la integridad de la red.

Procedimiento

El procedimiento metodológico se desarrolló en varias fases articuladas con los objetivos del trabajo:

- Recolección y organización de la información: durante la pasantía se recopilaron de manera sistemática los reportes, listados, capturas y

evidencias generados por Azure Entra ID, Qualys, CrowdStrike, SAP y las herramientas asociadas a la gestión de red, así como las matrices y documentos requeridos por revisoría fiscal y auditoría interna. Esta información se almacenó en las rutas institucionales definidas por el área de Seguridad Informática.

- Clasificación de actividades y controles: posteriormente, las actividades desarrolladas se agruparon según los cuatro ejes planteados en los objetivos específicos: monitoreo de identidades en la nube, gestión de vulnerabilidades y alertas, optimización de permisos en SAP y verificación de integridad de la red. Para cada eje se identificaron los procesos ejecutados, los controles aplicados y las evidencias disponibles.

- Análisis comparativo con el marco teórico: en esta fase se contrastaron las prácticas observadas en Colsubsidio con los conceptos y buenas prácticas descritos en el marco teórico sobre seguridad de la información, IAM, autenticación multifactor, gestión de vulnerabilidades, EDR, seguridad en ERP y seguridad de red. Esto permitió evaluar en qué medida los controles implementados se alinean con principios como la tríada CIA, el principio de mínimo privilegio y la segregación de funciones.

- Sistematización de la experiencia y elaboración de resultados: finalmente, se documentó de forma ordenada el conjunto de actividades, hallazgos y mejoras logradas, relacionando cada una con los objetivos específicos y con los requerimientos de la organización y de los entes de control. A partir de esta sistematización se construyeron los capítulos de desarrollo del trabajo, resultados, análisis y conclusiones, que reflejan el aporte de los controles de ciberseguridad y gestión de identidades al fortalecimiento de la seguridad informática en Colsubsidio.

Tipo de investigación

El presente trabajo corresponde a una investigación de tipo descriptivo, ya que se enfoca en documentar y explicar las actividades realizadas durante el desarrollo de la práctica profesional. Este tipo de investigación permite detallar los procesos, herramientas y procedimientos utilizados en el área de ciberseguridad de la organización, así como analizar su importancia dentro de la gestión de seguridad de la información.

A través del enfoque descriptivo se busca identificar los principales procesos relacionados con la gestión de accesos a sistemas empresariales, el monitoreo de vulnerabilidades y la utilización de herramientas tecnológicas de seguridad. Asimismo, se pretende evidenciar la manera en que estos procesos contribuyen al fortalecimiento de los controles de seguridad dentro de la organización.

Método de investigación

Para el desarrollo de la monografía se empleó el método analítico–descriptivo, el cual permitió examinar cada una de las actividades realizadas durante la práctica profesional y analizar su relación con los conceptos teóricos abordados en el marco conceptual de la investigación.

Este método consiste en descomponer el proceso general de la práctica profesional en diferentes actividades específicas, tales como la gestión de accesos a sistemas, el análisis de vulnerabilidades, el monitoreo de eventos de seguridad y el uso de herramientas tecnológicas especializadas. Posteriormente, estas actividades fueron analizadas con el propósito de comprender su impacto en la seguridad de los sistemas de información dentro de la organización.

Técnicas de recolección de información

Para la elaboración de la presente monografía se emplearon diversas técnicas de recolección de información que permitieron documentar las actividades desarrolladas durante la práctica profesional. Entre las principales técnicas utilizadas se encuentran:

1. Observación directa: La observación directa permitió analizar de manera detallada los procesos y actividades desarrollados dentro del área de ciberseguridad de la organización. A través de esta técnica fue posible identificar los procedimientos utilizados para la gestión de accesos, la administración de herramientas de seguridad y el monitoreo de posibles vulnerabilidades en los sistemas tecnológicos.

2. Revisión documental: Se realizó una revisión de documentos internos, manuales técnicos y documentación relacionada con las herramientas tecnológicas utilizadas dentro de la organización. Esta revisión permitió comprender el funcionamiento de

los sistemas utilizados para la gestión de seguridad informática y su aplicación dentro de los procesos empresariales.

3. Registro de actividades: Durante el desarrollo de la práctica profesional se llevó un registro de las actividades realizadas, lo que permitió documentar los procesos ejecutados, las herramientas utilizadas y los resultados obtenidos en cada una de las tareas asignadas. Este registro sirvió como base para el análisis y descripción de la experiencia desarrollada durante el periodo de pasantía.

Herramientas tecnológicas utilizadas durante la pasantía

SAP Logon 64: Es una herramienta que permite el acceso y la administración de los sistemas SAP dentro de una organización. A través de esta plataforma se gestionan usuarios, roles, perfiles y transacciones, lo que facilita el control de accesos a los diferentes módulos y sistemas empresariales. Su uso es fundamental para garantizar la correcta asignación de permisos, aplicar el principio de mínimo privilegio y asegurar la segregación de funciones. El uso de SAP Logon 64 en una empresa es beneficioso porque permite centralizar la gestión de identidades y accesos a sistemas críticos, mejorar la trazabilidad de las acciones realizadas por los usuarios y cumplir con requisitos de auditoría y control interno. Además, contribuye a reducir riesgos asociados a accesos no autorizados, errores operativos y fraudes internos.

Azure Entra ID: Es el servicio de gestión de identidades y accesos en la nube de Microsoft, anteriormente conocido como Azure Active Directory. Esta herramienta permite administrar usuarios, grupos, dispositivos y políticas de acceso, integrando mecanismos de seguridad como la autenticación multifactor (MFA) y el control de accesos condicionales. Su implementación en una empresa es altamente recomendable debido a que fortalece la seguridad de las identidades digitales, reduce el riesgo de accesos no autorizados y facilita la administración centralizada de usuarios tanto en entornos locales como en la nube. Azure Entra ID también mejora la experiencia del usuario al permitir accesos seguros y controlados a múltiples aplicaciones, apoyando los procesos de transformación digital y trabajo remoto.

Qualys: Es una plataforma de gestión de vulnerabilidades que permite identificar, analizar y clasificar debilidades de seguridad en infraestructuras tecnológicas y aplicaciones web. A través de escaneos automatizados, la herramienta detecta fallas de configuración, vulnerabilidades conocidas y riesgos potenciales que

podrían ser explotados por atacantes. El uso de Qualys en una empresa es fundamental para mantener una postura de seguridad proactiva, ya que permite anticiparse a posibles ataques y priorizar acciones de remediación según el nivel de riesgo. Además, facilita el cumplimiento de estándares y normativas de seguridad, aporta visibilidad continua sobre el estado de la infraestructura y reduce el impacto de incidentes de seguridad.

CrowdStrike: Es una plataforma de detección y respuesta ante amenazas (EDR) basada en la nube, diseñada para proteger equipos y servidores frente a ataques avanzados. La herramienta analiza comportamientos en tiempo real, detecta actividades sospechosas y genera alertas de seguridad que permiten una respuesta rápida ante incidentes. Su implementación en una empresa es altamente beneficiosa porque mejora la capacidad de detección temprana de amenazas, minimiza el tiempo de respuesta ante incidentes y reduce el impacto de ataques cibernéticos. CrowdStrike permite a las organizaciones fortalecer su estrategia de seguridad, proteger activos críticos y mantener la continuidad del negocio frente a un entorno de amenazas cada vez más sofisticado.

HERRAMIENTA	ÁREA	DESCRIPCIÓN DE USO	ACTIVIDADES REALIZADAS
SAP Logon 64	Gestión de Identidades	Plataforma utilizada para la administración de usuarios, roles y transacciones en los sistemas corporativos.	Monitoreo de usuarios no genéricos; validación de estados de cuentas; revisión de roles y transacciones; identificación de transacciones críticas; eliminación de más de mil roles; controles solicitados por revisoría fiscal; generación de evidencias mediante las transacciones SUIM, SU24 y SE16N para los sistemas ERP, CRM, PSP e IHP.
Azure Entra ID	Ciberseguridad	Herramienta de gestión de identidades en la nube para el control de accesos y autenticación.	Monitoreo del estado de usuarios; validación de habilitación de cuentas; verificación de autenticación multifactor (MFA); análisis de últimos accesos y ubicaciones; habilitación de MFA a usuarios; elaboración de informes quincenales para los dominios de Colsubsidio y CET Colsubsidio.
Qualys	Ciberseguridad	Plataforma de escaneo y gestión de vulnerabilidades.	Ejecución de escaneos de vulnerabilidades para las 24 páginas

			web de Colsubsidio; identificación y clasificación de vulnerabilidades según nivel de riesgo; documentación de resultados y almacenamiento de evidencias en las rutas definidas por la organización.
CrowdStrike	Ciberseguridad	Herramienta de detección y respuesta ante amenazas (EDR).	Monitoreo y análisis de alertas de seguridad; evaluación de eventos para determinar si representaban una amenaza real; escalamiento de incidentes críticos conforme a los procedimientos establecidos para la protección de la red corporativa.

Tabla 1. Herramientas tecnológicas utilizadas durante la pasantía

Fases de desarrollo de la práctica

El desarrollo de la práctica profesional se llevó a cabo en diferentes fases que permitieron la integración progresiva del practicante en las actividades del área de ciberseguridad.

Fase de inducción: Durante esta fase se realizó el proceso de inducción a la organización, donde se presentaron las políticas internas, los lineamientos de seguridad y las principales herramientas tecnológicas utilizadas dentro del área de tecnología.

Fase de aprendizaje y adaptación: En esta etapa se adquirieron conocimientos sobre el funcionamiento de las herramientas de seguridad utilizadas por la organización, así como los procedimientos relacionados con la gestión de accesos y el monitoreo de sistemas.

Fase de ejecución de actividades: En esta fase se desarrollaron las actividades asignadas dentro del área de ciberseguridad, participando en procesos relacionados con la gestión de identidades, control de accesos a sistemas empresariales, revisión de vulnerabilidades y análisis de eventos de seguridad.

Fase de análisis y documentación: Finalmente, se realizó el análisis de las actividades desarrolladas durante la práctica profesional, documentando los procesos realizados, las herramientas utilizadas y los resultados obtenidos durante la experiencia laboral.

8. DESARROLLO DEL TRABAJO

8.1. Monitoreo de identidades en la nube con Azure Entra ID

En relación con el primer objetivo específico, el trabajo se centró en el monitoreo sistemático de las identidades en la nube de Colsubsidio y CET Colsubsidio a través de Azure Entra ID, con el propósito de fortalecer los controles de autenticación y acceso a los servicios corporativos. Durante el periodo de práctica se ejecutaron revisiones periódicas del estado de habilitación de las cuentas de usuario, verificando si se encontraban activas, bloqueadas o pendientes de acción administrativa, y se analizaron los registros de actividad asociados a últimos inicios de sesión y ubicaciones de conexión.

A partir de los reportes generados por la plataforma se construyeron informes quincenales, en los que se consolidaba la información de ambos dominios, destacando usuarios con comportamientos atípicos, cuentas sin autenticación multifactor (MFA) configurada y accesos desde ubicaciones geográficas no habituales. Estos informes se socializaban con el equipo de Seguridad Informática para que, de acuerdo con los procedimientos internos, se gestionaran acciones como la activación de MFA, el bloqueo preventivo de cuentas o la verificación con las áreas responsables cuando se identificaban situaciones de riesgo.

Adicionalmente, se apoyó la habilitación progresiva de MFA para usuarios que aún no contaban con este mecanismo, registrando los cambios realizados y manteniendo evidencias de las configuraciones aplicadas. Esta labor contribuyó a incrementar el porcentaje de cuentas protegidas con múltiples factores de autenticación y a alinear la operación de Colsubsidio con las buenas prácticas de gestión de identidades en entornos cloud, reduciendo la probabilidad de accesos indebidos por robo o filtración de credenciales.

8.1.1. Descripción de las actividades

Una de las principales labores fue el monitoreo y gestión de usuarios mediante Azure Entra ID, donde se verifica el estado de habilitación de las cuentas, la configuración de autenticación multifactor (MFA), los últimos accesos registrados y las ubicaciones desde las cuales se realizaban las conexiones. Esta actividad se ejecutó para los usuarios pertenecientes a los dominios de Colsubsidio y CET Colsubsidio, generando informes quincenales con la información recolectada.

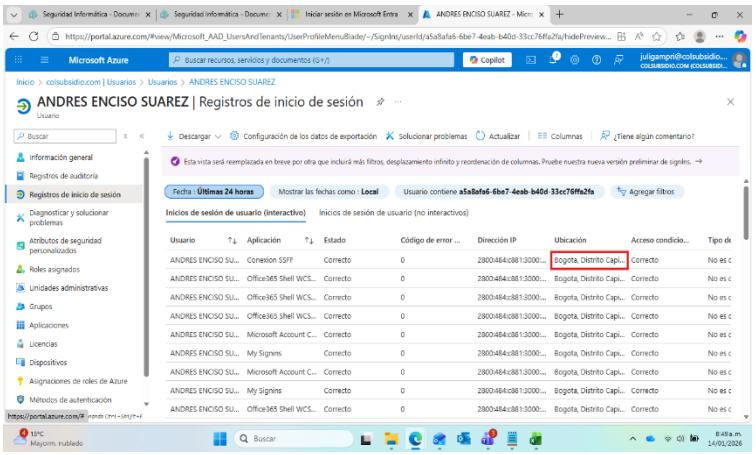


Figura 1. Informe quincenal de estado de cuentas y configuración de MFA en Azure Entra ID. Fuente: elaboración propia.

8.2. Gestión de vulnerabilidades web y respuesta ante alertas de seguridad

En cumplimiento del segundo objetivo específico, se desarrollaron actividades orientadas a la identificación y análisis de vulnerabilidades en los portales web de Colsubsidio, así como a la evaluación de alertas de seguridad generadas en los endpoints corporativos. Para ello se utilizó la herramienta Qualys, mediante la cual se ejecutaron escaneos de seguridad sobre veinticuatro sitios web de la organización, obteniendo reportes detallados de debilidades técnicas clasificadas por niveles de severidad.

Los resultados de los escaneos fueron documentados y almacenados en las rutas definidas por el área de Seguridad Informática, organizando las vulnerabilidades según su criticidad y afectación potencial sobre la confidencialidad, integridad y disponibilidad de la información. Esta clasificación permitió priorizar las debilidades más relevantes, identificar patrones recurrentes (como versiones desactualizadas o configuraciones inseguras) y suministrar insumos claros a los equipos encargados de la remediación.

De manera complementaria, se participó en la gestión de alertas de ciberseguridad generadas por CrowdStrike, plataforma EDR desplegada en la infraestructura de la organización. En este frente, el trabajo consistió en revisar los eventos reportados, diferenciar entre actividades informativas y posibles incidentes, y escalar los casos que representaban una amenaza real para la red corporativa, conforme a los procedimientos internos establecidos. Esta labor incluyó la consulta específica de direcciones IP sospechosas mediante la interfaz de línea de comandos, con el fin

de obtener mayor contexto sobre los comportamientos observados y sustentar las decisiones de respuesta.

Finalmente, se llevaron a cabo pruebas de acceso web basadas en la matriz de categorías y subcategorías FortiGuard, verificando que los sitios restringidos por política estuvieran siendo efectivamente bloqueados por los mecanismos de filtrado. Cuando se detectaban diferencias entre la matriz de referencia y el comportamiento real de la navegación, se elaboraban informes de las inconsistencias y se escalaban al proveedor correspondiente para su corrección, contribuyendo a cerrar brechas entre la política definida y su implementación tecnológica.

8.2.1. Descripción de las actividades

Gestión y análisis de alertas de ciberseguridad generadas por la herramienta CrowdStrike, evaluando si los eventos representaban una amenaza real para la red corporativa. En los casos críticos, los incidentes eran escalados conforme a los procedimientos establecidos, contribuyendo a la oportuna respuesta ante posibles riesgos de seguridad.

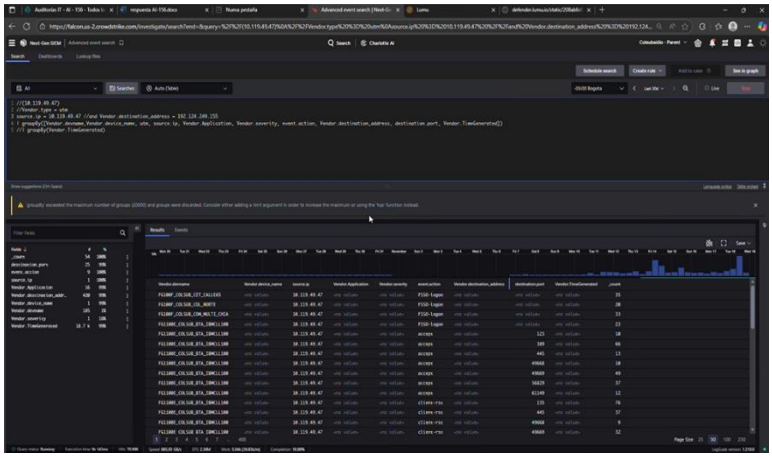


Figura 2. Registro de alerta de seguridad en CrowdStrike para endpoint corporativo. Fuente: elaboración propia.

Asimismo, se realizó el monitoreo y documentación de vulnerabilidades de las 24 páginas web de Colsubsidio mediante la herramienta Qualys, ejecutando escaneos de seguridad y clasificando las vulnerabilidades según el nivel de riesgo definido por la plataforma.

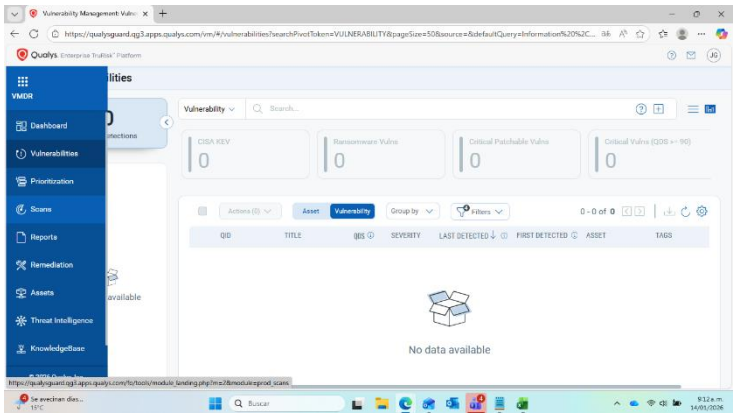


Figura 3. Resultado de escaneo de vulnerabilidades de portal web en Qualys con clasificación por niveles de riesgo.
Fuente: elaboración propia.

8.3. Optimización de permisos y control de accesos en sistemas SAP

El tercer objetivo específico se enfocó en la optimización de permisos en los sistemas SAP utilizados por Colsubsidio, con énfasis en la depuración de roles obsoletos y en el control mensual de transacciones críticas. En una primera etapa, se realizó el monitoreo de usuarios no genéricos en SAP Logon para los sistemas ERP, CRM, PSP e IHP, validando el estado de las cuentas (activas o inactivas), los perfiles asignados y las transacciones a las que tenían acceso.

A partir de la información obtenida mediante transacciones como SUIM, SU24 y SE16N, se efectuaron cruces de información para identificar usuarios con acceso a las 113 transacciones clasificadas como críticas por la organización, verificando la pertinencia de dichos permisos frente a las funciones del usuario. Cuando se detectaban asignaciones injustificadas o riesgosas, los casos eran escalados a los responsables de proceso para su revisión y eventual ajuste.

En paralelo, se apoyó un proceso de eliminación de más de mil roles en SAP, orientado a depurar accesos innecesarios que se habían acumulado con el tiempo y que ya no respondían a la estructura organizacional vigente. Esta depuración se realizó de manera controlada, revisando el uso histórico de los roles, su impacto en los usuarios y documentando las acciones ejecutadas para mantener trazabilidad. Asimismo, se actualizaron matrices de roles satélite y se revisaron mensualmente usuarios con privilegios elevados (por ejemplo, con accesos como SAP_ALL, SAP_NEW o transacciones de administración), verificando que contaran con las justificaciones y aprobaciones correspondientes.

Como parte de los requerimientos de revisoría fiscal, se generaron evidencias periódicas sobre usuarios críticos y controles específicos sobre cuentas técnicas, cumpliendo los plazos establecidos y asegurando que las matrices de acceso SAP y NO SAP estuvieran validadas antes de la salida a producción de nuevos proyectos. Estas acciones consolidaron el principio de mínimo privilegio, reforzaron la segregación de funciones y redujeron la exposición a errores operativos y posibles fraudes en los sistemas de misión crítica.

8.3.1. Descripción de las actividades

Se realizó el monitoreo de usuarios no genéricos en SAP Logon, validando su estado (activo o inactivo), los perfiles y transacciones asignadas, y realizando cruces de información para identificar usuarios con transacciones críticas dentro de las 113 transacciones definidas por la organización. Estas actividades se ejecutaron para los sistemas ERP, CRM, PSP e IHP, utilizando herramientas como SAP Logon 64, SUIM, SU24 y SE16N. Cuando se identificaba que un usuario tenía asignada una transacción crítica, el caso era escalado al responsable correspondiente para su validación y gestión.

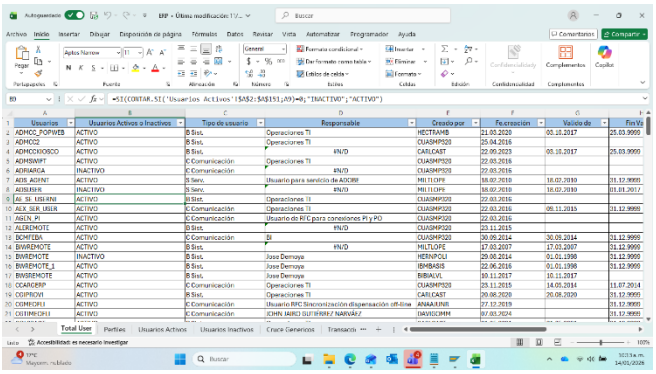


Figura 4. Listado de usuarios con transacciones críticas identificados mediante SUIM en SAP. Fuente: elaboración propia.

Otras actividades incluyeron la validación de matrices de acceso NO SAP para proyectos y procesos, requisito indispensable para la salida a producción de nuevas iniciativas, la actualización de la matriz de roles satélite SAP a partir de información obtenida del OIM, y la revisión mensual de usuarios con transacciones de alto privilegio como SAP_ALL, SAP_NEW y S_A.SYSTEM, verificando su debida justificación.

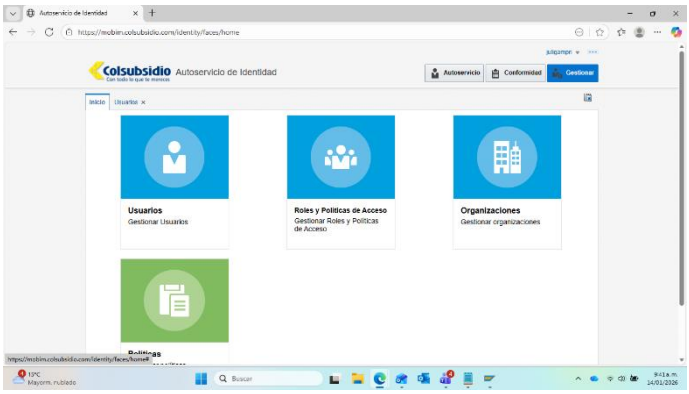


Figura 5 se evidencia el proceso de eliminación de roles obsoletos, como parte de la depuración de accesos en los sistemas ERP, CRM, PSP e IHP.
Fuente: elaboración propia.

8.4. Verificación de la integridad de la red y generación de evidencias para revisoría fiscal

El cuarto objetivo específico se orientó a verificar la integridad de la infraestructura de red y la reputación de los servicios expuestos, así como a producir evidencias formales para los procesos de auditoría y revisoría fiscal. En este contexto, una de las actividades principales fue la validación de direcciones IP de firewalls y servidores contra listas negras (blacklists) proporcionadas al área de Seguridad Informática.

El procedimiento consistió en contrastar periódicamente las IP de la organización con los registros de diversas listas de reputación, identificando si alguno de los rangos o direcciones se encontraba reportado por envío de correo no deseado, actividad sospechosa u otros comportamientos considerados de riesgo. Cuando se detectaba una IP incluida en listas negras, se gestionaba la respectiva solicitud de retiro ante los proveedores de servicios de internet (Claro y UNE), aportando la información requerida y haciendo seguimiento hasta la confirmación de la exclusión, con el fin de evitar afectaciones en la disponibilidad y confiabilidad de los servicios tecnológicos de Colsubsidio.

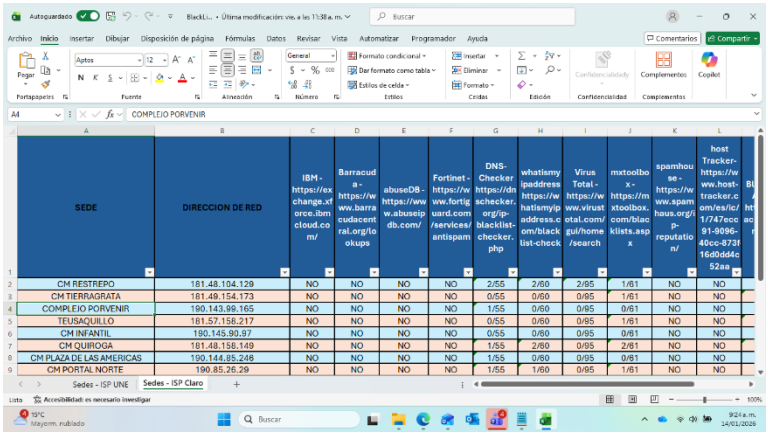
De forma complementaria, se elaboró y mantuvo un inventario general de dispositivos de conectividad, incluyendo access points, firewalls, servidores, switches, gestores de firewall y sistemas de telefonía IP, registrando datos como direcciones IP, tipo de dispositivo, marca y proveedor. Este inventario permitió mejorar la visibilidad de la infraestructura de red y se convirtió en un insumo clave

para la gestión de activos de información y para la trazabilidad de cambios y eventos de seguridad.

Finalmente, se generaron informes mensuales y quincenales de evidencias sobre usuarios con privilegios elevados y sobre la ejecución de controles definidos por revisoría fiscal, documentando de manera estructurada los resultados de las revisiones y las acciones tomadas. Estos informes se almacenaron en las rutas institucionales designadas y se pusieron a disposición de los equipos de auditoría, demostrando el cumplimiento de los controles definidos y reforzando la gobernanza sobre los accesos privilegiados y la operación de la red corporativa.

8.4.1. Descripción de las actividades

Se realizo la validación de direcciones IP correspondientes a firewalls y servidores de la organización, con el fin de identificar si estas se encontraban incluidas en listas negras (blacklists) suministradas. En los casos en los que una IP era detectada en una blacklist, se gestionaba la solicitud para su retiro ante los proveedores de servicios de internet Claro y UNE, asegurando la continuidad y correcta operación de los servicios tecnológicos.



SEDE	DIRECCION DE RED	IBM - https://exchange.xforce.ibmcloud.com/	Barracuda - https://www.barracudacentral.org/lookups	abuseDB - https://www.abuseipdb.com/	Fortinet - https://www.fortiguard.com/services/antispam	DNS-Checker https://dnschecker.org/ip-blacklist-checker.php	whatismyipaddress https://whatismyipaddress.com/blacklist-check	Virus Total - https://www.virustotal.com/gui/home/search	mxtoolbox - https://mxtoolbox.com/blacklists.aspx	spamhouse - https://www.spamhaus.org/sp-reputation/	host Tracker- https://www.host-tracker.com/es/ic/1/747ecc91-9896-40cc-873f16d0dd4c52aa
CM RESTREPO	181.48.104.129	NO	NO	NO	NO	2/55	2/60	2/95	1/61	NO	NO
CM TIERRAGRATA	181.49.154.173	NO	NO	NO	NO	0/55	0/60	0/95	1/61	NO	NO
COMPLEJO PORVENIR	190.143.99.165	NO	NO	NO	NO	1/55	0/60	0/95	0/61	NO	NO
TEUSAQUILLO	181.57.158.217	NO	NO	NO	NO	0/55	0/60	0/95	1/61	NO	NO
CM INFANTIL	190.145.90.97	NO	NO	NO	NO	0/55	0/60	0/95	0/61	NO	NO
CM QUIROGA	181.48.158.149	NO	NO	NO	NO	1/55	2/60	0/95	2/61	NO	NO
CM PLAZA DE LAS AMERICAS	190.144.85.246	NO	NO	NO	NO	1/55	0/60	0/95	0/61	NO	NO
CM PORTAL NORTE	190.85.26.29	NO	NO	NO	NO	1/55	1/60	0/95	1/61	NO	NO

Figura 6. Verificación de direcciones IP de firewalls en listas negras.
Fuente: elaboración propia.

Otra actividad relevante fue la elaboración de un inventario general de dispositivos de conectividad, incluyendo access points, firewalls, servidores, switches, gestores de firewall y sistemas VoIP, donde se documentó información como dirección IP, marca, tipo de dispositivo y proveedor. Este inventario permitió fortalecer la visibilidad de la infraestructura tecnológica y apoyar la gestión de activos de información.

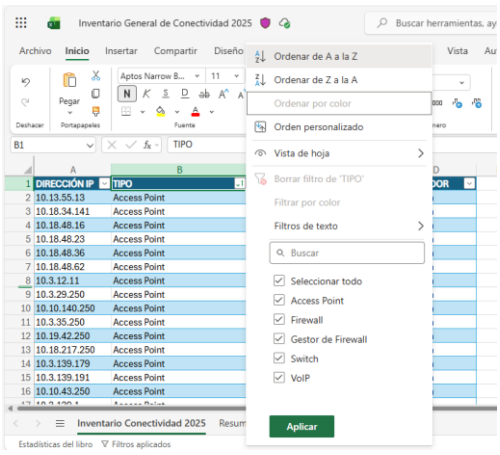


Figura 7. Extracto del inventario de dispositivos de conectividad (firewalls, switches, servidores). Fuente: elaboración propia.

9. RESULTADOS Y ANÁLISIS

Resultados obtenidos:

Como resultado del desarrollo de las actividades contempladas en los cuatro objetivos específicos, se logró fortalecer de manera tangible el control y el monitoreo de los procesos relacionados con la ciberseguridad y la gestión de identidades y accesos dentro de Colsubsidio. La ejecución constante de tareas de seguimiento, validación y documentación permitió consolidar un conjunto de evidencias estructuradas que respaldan los controles definidos por la Gerencia de Tecnología y por los entes de auditoría interna y externa.

En el ámbito del monitoreo de identidades en la nube, la generación de informes quincenales a partir de Azure Entra ID permitió identificar cuentas sin autenticación multifactor (MFA) configurada, accesos desde ubicaciones geográficas no habituales y usuarios con patrones de inicio de sesión atípicos. Estos hallazgos facilitaron la activación progresiva de MFA en un número significativo de cuentas y la adopción de medidas preventivas, como el bloqueo temporal de usuarios o la verificación con las áreas responsables cuando se detectaban comportamientos de riesgo.

En el componente de gestión de vulnerabilidades y respuesta ante amenazas, los escaneos realizados con Qualys sobre veinticuatro portales web de Colsubsidio permitieron identificar y documentar múltiples debilidades técnicas, clasificadas por nivel de severidad y asociadas a recomendaciones de remediación. Paralelamente, el uso de CrowdStrike posibilitó una respuesta más estructurada frente a los eventos de seguridad en endpoints, diferenciando entre alertas informativas y verdaderos incidentes que debían escalarse conforme a los procedimientos internos, lo que contribuyó a mejorar los tiempos y la calidad de la reacción institucional ante posibles ataques.

Respecto a la optimización de permisos en SAP, el monitoreo de usuarios no genéricos en los sistemas ERP, CRM, PSP e IHP permitió detectar accesos innecesarios, transacciones críticas asignadas sin justificación clara y acumulación de roles obsoletos. Este trabajo derivó en la eliminación de más de mil roles en SAP, la actualización de matrices de roles satélite y el control sistemático de las ciento trece transacciones críticas definidas por la organización, disminuyendo la exposición a riesgos de fraude interno, errores operativos y hallazgos recurrentes en auditoría.

En cuanto a la verificación de la integridad de la red y la reputación de las direcciones IP, la revisión periódica de IP de firewalls y servidores frente a listas negras permitió detectar oportunamente aquellos casos en los que la infraestructura de Colsubsidio había sido reportada, gestionando su retiro ante los proveedores de servicios de internet y evitando afectaciones prolongadas en la disponibilidad de los servicios tecnológicos. Estas actividades se complementaron con la elaboración de un inventario general de dispositivos de conectividad y con la generación de informes mensuales y quincenales de evidencias para revisoría fiscal sobre usuarios con privilegios elevados, fortaleciendo la trazabilidad y la gobernanza de los accesos privilegiados.

En conjunto, los resultados demuestran que las actividades desarrolladas durante la pasantía no solo tuvieron un impacto operativo inmediato, sino que también aportaron insumos valiosos para la consolidación de los procesos de seguridad de la información y de cumplimiento normativo de la organización.

Análisis de los resultados:

El análisis de los resultados evidencia que las actividades desarrolladas durante la práctica profesional se alinean con los principios y buenas prácticas establecidos en estándares internacionales de seguridad de la información, como la norma ISO/IEC 27001:2022 y los lineamientos del NIST Cybersecurity Framework.

En el componente de gestión de identidades, el monitoreo de usuarios en Azure Entra ID, junto con la implementación de autenticación multifactor (MFA), responde directamente a los controles de acceso definidos en ISO 27001, específicamente en el dominio de control de accesos (Annex A), donde se establece la necesidad de garantizar mecanismos de autenticación robustos para prevenir accesos no autorizados. La identificación de cuentas sin MFA y la detección de accesos desde ubicaciones atípicas evidencian la aplicación de controles preventivos orientados a la protección de la confidencialidad de la información, uno de los pilares de la tríada CIA.

Asimismo, el análisis de patrones de acceso y la gestión de usuarios activos e inactivos se relaciona con el concepto de gestión del ciclo de vida de identidades (Identity Lifecycle Management), el cual es fundamental dentro de los modelos IAM. Este proceso permite reducir riesgos asociados a cuentas huérfanas o accesos indebidos, alineándose con el principio de mínimo privilegio, ampliamente recomendado por marcos como NIST SP 800-53.

En cuanto a la gestión de vulnerabilidades, los escaneos realizados con Qualys sobre los portales web de la organización se fundamentan en las prácticas recomendadas por el modelo de gestión de vulnerabilidades, el cual establece la necesidad de identificar, clasificar y mitigar debilidades en los sistemas antes de que puedan ser explotadas. La clasificación de vulnerabilidades por niveles de severidad se relaciona directamente con el estándar CVSS (Common Vulnerability Scoring System), el cual permite priorizar las acciones de mitigación según el impacto potencial.

Por su parte, el uso de CrowdStrike como herramienta de detección y respuesta ante amenazas (EDR) se alinea con los controles de monitoreo continuo y respuesta a incidentes establecidos en el NIST Cybersecurity Framework, particularmente en las funciones de “Detect” y “Respond”. La diferenciación entre alertas informativas e incidentes reales evidencia la implementación de procesos estructurados de análisis y escalamiento, lo cual mejora la capacidad de respuesta ante amenazas en tiempo real.

En el ámbito de los sistemas ERP, específicamente en SAP, la eliminación de roles obsoletos y el control de transacciones críticas se fundamentan en el principio de segregación de funciones (SoD) y en el principio de mínimo privilegio. Estas prácticas son esenciales para prevenir fraudes internos y errores operativos, y están alineadas con los controles de auditoría y gobierno de accesos definidos en marcos como COBIT y las buenas prácticas de seguridad en sistemas empresariales.

Finalmente, la verificación de direcciones IP en listas negras y la gestión de su retiro se relaciona con los controles de seguridad de red y gestión de la reputación de la infraestructura tecnológica. Este proceso contribuye a garantizar la disponibilidad de los servicios, uno de los pilares de la tríada CIA, y se alinea con las recomendaciones de seguridad perimetral establecidas en estándares internacionales.

En conjunto, los resultados obtenidos demuestran que la integración de herramientas como Azure Entra ID, Qualys, CrowdStrike y SAP, junto con la aplicación de buenas prácticas de seguridad, permite fortalecer la postura de seguridad de la organización, evidenciando la importancia de una estrategia integral basada en estándares y marcos de referencia reconocidos a nivel internacional.

10. CONCLUSIONES

La experiencia desarrollada durante la práctica profesional permitió evidenciar que la implementación de controles de ciberseguridad y gestión de identidades en la organización se encuentra alineada con estándares internacionales como ISO/IEC 27001 y el NIST Cybersecurity Framework, lo que demuestra que las actividades realizadas no solo tienen un impacto operativo, sino también un sustento metodológico y normativo dentro de la seguridad de la información.

El desarrollo de actividades orientadas al control de accesos privilegiados, la depuración de roles, la validación de matrices de acceso y la generación de evidencias para auditoría permitió fortalecer la trazabilidad y la gobernanza de los sistemas de información. Estos resultados reflejan que una gestión adecuada de identidades reduce significativamente los riesgos asociados a errores de configuración, accesos indebidos y posibles incumplimientos ante entes de control y revisoría fiscal.

La sistematización de las actividades desarrolladas en el área de Seguridad Informática de Colsubsidio permitió demostrar que la articulación entre ciberseguridad, gestión de identidades, gestión de vulnerabilidades y seguridad de red es un factor determinante para la protección efectiva de los activos tecnológicos y el cumplimiento de los lineamientos normativos de la organización. El monitoreo constante de usuarios, accesos, roles, transacciones críticas, vulnerabilidades web y reputación de direcciones IP evidenció que la seguridad de la información depende en gran medida de controles preventivos, seguimiento continuo y una adecuada administración del ciclo de vida de las identidades digitales.

Los resultados obtenidos en la gestión de identidades, particularmente en la implementación de autenticación multifactor, el monitoreo de accesos y la depuración de roles en sistemas SAP, evidencian la aplicación efectiva del principio de mínimo privilegio y la segregación de funciones. Estos principios son fundamentales en la prevención de accesos indebidos y en el fortalecimiento del control interno, tal como lo establecen las buenas prácticas de IAM y los marcos de gobierno de TI.

En el componente de ciberseguridad, la combinación del monitoreo de identidades en Azure Entra ID, la ejecución de escaneos con Qualys sobre veinticuatro portales web y la gestión de alertas de CrowdStrike demostró que la detección temprana de vulnerabilidades y amenazas es posible cuando se integran adecuadamente las

capacidades de IAM, gestión de vulnerabilidades y EDR con procesos claros de análisis y escalamiento. Al mismo tiempo, la verificación de direcciones IP en listas negras y la gestión de su retiro ante los proveedores de servicios de internet confirmó la importancia de la reputación de la infraestructura de red para garantizar la disponibilidad y confiabilidad de los servicios tecnológicos frente a usuarios internos y externos.

Desde la perspectiva formativa, la experiencia de pasantía permitió consolidar competencias técnicas en ciberseguridad e IAM, así como habilidades analíticas y de documentación de procesos bajo estándares organizacionales, reafirmando el rol estratégico del profesional en seguridad de la información dentro de organizaciones complejas. El trabajo realizado no solo generó beneficios operativos inmediatos para Colsubsidio, sino que también produjo un marco de referencia práctico que puede ser aprovechado por la Gerencia de Tecnología para futuras iniciativas de mejora y por la academia como ejemplo de aplicación de los fundamentos teóricos en un contexto real de negocio.

BIBLIOGRAFÍA

[1] International Organization for Standardization, ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements, Ginebra, Suiza, 2022. [En línea]. Disponible en: https://www.iso.org/standard/27001.html. [Accedido: 18-mar-2026].

[2] GRC Solutions, “ISO/IEC 27001:2022 – The Information Security Management …,” 2025. [En línea]. Disponible en: https://grcsolutions.io/iso27001/. [Accedido: 18-mar-2026].

[3] Oracle, “Identity and Access Management (IAM),” 2023. [En línea]. Disponible en: https://www.oracle.com/latam/security/identity-management/. [Accedido: 18-mar-2026].

[4] Oracle, “Identity and Access Management (IAM) Defined,” 2021. [En línea]. Disponible en: https://www.oracle.com/security/identity-management/what-is-iam/. [Accedido: 18-mar-2026].

[5] Check Point, “¿Qué es la gestión de identidades y accesos (IAM)?,” 2022. [En línea]. Disponible en: (sitio de Check Point – sección Cyber Hub IAM). [Accedido: 18-mar-2026].

[6] Tenable, “¿Qué es la gestión de identidades y acceso (IAM)?,” 2025. [En línea]. Disponible en: (sitio de Tenable – cybersecurity guide / IAM). [Accedido: 18-mar-2026].

[7] Fortinet, “Administración de identidad y acceso (IAM),” s. f. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/identity-and-access-management. [Accedido: 18-mar-2026].

[8] ABC Xperts, “¿Qué es la tríada en Seguridad de la Información?,” 2024. [En línea]. Disponible en: (blog de ABC Xperts). [Accedido: 18-mar-2026].

[9] DataSunrise, “Confidencialidad, Integridad, Disponibilidad: Ejemplos Clave,” 2025. [En línea]. Disponible en: (sitio de DataSunrise – knowledge center). [Accedido: 18-mar-2026].

[10] Silikn, “Tríada CIA: un marco de principios para definir políticas de seguridad,” 2024. [En línea]. Disponible en: (blog de Silikn). [Accedido: 18-mar-2026].

[11] Computer Weekly, “¿Qué es autenticación multifactor o MFA?,” 2021. [En línea]. Disponible en: (glosario en español de Computer Weekly). [Accedido: 18-mar-2026].

[12] Fortinet, “¿Qué es la autenticación multifactor (MFA)?,” s. f. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/multi-factor-authentication. [Accedido: 18-mar-2026].

[13] Mitek Systems, “¿Qué es la autenticación multifactor?,” 2026. [En línea]. Disponible en: (blog de Mitek). [Accedido: 18-mar-2026].

[14] INCIBE-CERT, “CVSS v4.0: avanzando en la evaluación de vulnerabilidades,” 2023. [En línea]. Disponible en: https://www.incibe.es/incibe-cert/blog/cvss-v40-avanzando-en-la-evaluacion-de-vulnerabilidades. [Accedido: 18-mar-2026].

[15] TuxCare, “La transición a CVSS v4.0: lo que necesita saber,” 2025. [En línea]. Disponible en: https://tuxcare.com/es/blog/cvss-v4-0. [Accedido: 18-mar-2026].

[16] Hispasec – Una al día, “CVSS 4.0: Nueva versión de evaluación de vulnerabilidades,” 2023. [En línea]. Disponible en: https://unaaldia.hispasec.com/2023/11/cvss-4-0-nueva-version-de-evaluacion-de-vulnerabilidades.html. [Accedido: 18-mar-2026].

[17] Trellix, “¿Qué es la detección y respuesta para endpoints (EDR)?,” 2024. [En línea]. Disponible en: (sitio de Trellix – security awareness / endpoint). [Accedido: 18-mar-2026].

[18] Trend Micro, “¿Qué es Endpoint Detection and Response (EDR)?,” 2025. [En línea]. Disponible en: https://www.trendmicro.com/es_mx/what-is/xdr/edr.html. [Accedido: 18-mar-2026].

[19] Kaspersky, “¿Qué es la EDR? Definición de Endpoint Detection and Response,” 2022. [En línea]. Disponible en: (resource center de Kaspersky). [Accedido: 18-mar-2026].

[20] Proofpoint, “¿Qué es EDR (Endpoint Detection and Response)?,” 2024. [En línea]. Disponible en: (Threat Reference de Proofpoint). [Accedido: 18-mar-2026].

[21] EvaluandoERP, “Seguridad del ERP y restricciones dentro del sistema,” 2024. [En línea]. Disponible en: https://www.evaluandoerp.com/sistema-de-gestion/sistema-erp/seguridad-y-restricciones-del-sistema/. [Accedido: 18-mar-2026].

[22] ComparaSoftware, “7 estándares de seguridad de un ERP: ¿tu proveedor los cumple?,” 2023. [En línea]. Disponible en: https://blog.comparasoftware.com/estandares-seguridad-erp/. [Accedido: 18-mar-2026].

[23] SkyPlanner, “La seguridad de ERP,” 2025. [En línea]. Disponible en: https://skyplanner.ai/es/recursos/la-seguridad-de-erp/. [Accedido: 18-mar-2026].

[24] Calipso, “Seguridad en el ERP,” 2025. [En línea]. Disponible en: https://www.calipso.com/articulos/seguridad-en-el-erp/. [Accedido: 18-mar-2026].

[25] GuruSIS, “Sistemas ERP con seguridad y protección de datos,” 2024. [En línea]. Disponible en: https://gurusis.com/seguridad-y-proteccion-de-datos-en-sistemas-erp/. [Accedido: 18-mar-2026].

[26] Z-Net, “Tutorial: cómo filtrar sitios por categorías y listas negras en Fortigate,” s. f. [En línea]. Disponible en: https://www.z-net.com.ar/blog-post/9-tutorial-como-filtrar-sitios-por-categorias-y-listas-negras-en-fortigate/. [Accedido: 18-mar-2026].

[27] Fortinet, “Servicio de filtrado web FortiGuard,” s. f. [En línea]. Disponible en: https://www.fortinet.com/lat/support/support-services/fortiguard-security-subscriptions/web-filtering. [Accedido: 18-mar-2026].

[28] Fortinet, “FortiGuard filter – FortiGate/FortiOS 7.6.5 Administration Guide,” 2025. [En línea]. Disponible en: https://docs.fortinet.com/document/fortigate/7.6.5/administration-guide/675558/fortiguard-filter. [Accedido: 18-mar-2026].

[29] FortiGuard, “Web Filter Categories,” s. f. [En línea]. Disponible en: https://www.fortiguard.com/webfilter/categories. [Accedido: 18-mar-2026].

[30] PowerDMARC, “Comprobador de listas negras: controle la reputación de su dominio,” 2025. [En línea]. Disponible en: https://powerdmarc.com/es/blacklist-monitoring-ip-check/. [Accedido: 18-mar-2026].

[31] Email Vendor Selection, “Las 7 mejores herramientas para comprobar la reputación IP,” 2026. [En línea]. Disponible en: (blog de EmailVendorSelection). [Accedido: 18-mar-2026].

[32] ZeroBounce, “Verificador gratuito de listas negras de IP y dominios,” s. f. [En línea]. Disponible en: https://www.zerobounce.net/es/blacklist-checker. [Accedido: 18-mar-2026].

[33] Mailjet, “Lista negra: qué es y cómo saber si tu IP está en una blacklist,” 2026. [En línea]. Disponible en: https://www.mailjet.com/es/blog/entregabilidad/blacklist/. [Accedido: 18-mar-2026].

[34] Benchmark Email, “Pasos a seguir cuando tu dirección IP está en la lista negra,” 2024. [En línea]. Disponible en: https://www.benchmarkemail.com/es/blog/pasos-a-seguir-cuando-su-direccion-de-ip-esta-en-la-lista-negra/. [Accedido: 18-mar-2026].

[35] COLSUBSIDIO, Organigrama Colsubsidio. Bogotá, D. C., Colsubsidio, s. f. [En línea]. Disponible en: https://www.colsubsidio.com/hubfs/documentos/colsubsidio/organigrama-colsubsidio.pdf. [Accedido: 20-ene-2026].

[36] Microsoft Corporation, Azure Entra ID Documentation. Redmond, WA, Microsoft, 2024. [En línea]. Disponible en: https://learn.microsoft.com. [Accedido: 20-ene-2026].

[37] SAP SE, SAP NetWeaver – User Administration and Authorization Concepts. Walldorf, Alemania, SAP SE, 2023. [En línea]. Disponible en: https://help.sap.com. [Accedido: 20-ene-2026].

[38] SAP SE, SAP Security Guide. Walldorf, Alemania, SAP SE, 2023. [En línea]. Disponible en: https://help.sap.com. [Accedido: 20-ene-2026].

[39] Qualys Inc., Qualys Vulnerability Management User Guide. Foster City, CA, Qualys Inc., 2024. [En línea]. Disponible en: https://www.qualys.com/documentation/. [Accedido: 20-ene-2026].

[40] CrowdStrike Inc., CrowdStrike Falcon Platform Documentation. Sunnyvale, CA, CrowdStrike, 2024. [En línea]. Disponible en: https://www.crowdstrike.com/resources/. [Accedido: 20-ene-2026].

[41] COLSUBSIDIO, Perfil organizacional de Colsubsidio. Bogotá, D. C., Colsubsidio, 2025. [En línea]. Disponible en: https://www.colsubsidio.com/quienes-somos/perfil-organizacional. [Accedido: 18-ene-2026].

[42] COLSUBSIDIO, "¿Quiénes somos?," Bogotá, D. C., Colsubsidio, 2026. [En línea]. Disponible en: https://www.colsubsidio.com/quienes-somos. [Accedido: 18-ene-2026].

[43] ABC Xperts, "¿Qué es la triada en Seguridad de la Información?," 2024. [En línea]. Disponible en: https://abcxperts.com/que-es-la-triada-en-seguridad-de-la-informacion/. [Accedido: 13-mar-2026].

[44] DataSunrise, "Confidencialidad, Integridad, Disponibilidad: Ejemplos Clave," 2025. [En línea]. Disponible en: https://www.datasunrise.com/es/centro-de-conocimiento/ejemplos-de-confidencialidad-integridad-disponibilidad/. [Accedido: 13-mar-2026].

[45] Ontek, "Tríada CID (Confidencialidad, Integridad y Disponibilidad)," 2019. [En línea]. Disponible en: https://www.ontek.net/que-es-triada-cid/. [Accedido: 13-mar-2026].

[46] Silikn, “Tríada CIA: Un marco de principios para definir políticas de seguridad,” 2024. [En línea]. Disponible en: https://www.silikn.com/2024/07/triada-cia-un-marco-de-principios-para.html. [Accedido: 13-mar-2026].

[47] Oracle, “Qué es Identity and Access Management (IAM),” 2024. [En línea]. Disponible en: https://www.oracle.com/latam/security/identity-management/what-is-iam/. [Accedido: 14-mar-2026].

[48] Fortinet, “¿Qué es la autenticación multifactor (MFA)?,” s. f. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/multi-factor-authentication. [Accedido: 14-mar-2026].

[49] Trend Micro, “¿Qué es el Common Vulnerability Scoring System (CVSS)?,” 2026. [En línea]. Disponible en: https://www.trendmicro.com/es_es/what-is/attack-surface/cvss-common-vulnerability-scoring-system.html. [Accedido: 15-mar-2026].

[50] Fortinet, “Sistema de puntuación de vulnerabilidades comunes (CVSS),” s. f. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/common-vulnerability-scoring-system. [Accedido: 15-mar-2026].

[51] Deusto Formación, “Gestionar la seguridad en SAP: accesos y autorizaciones,” 2018. [En línea]. Disponible en: https://www.deustoformacion.com/blog/gestion-empresas/gestionar-seguridad-sap-accesos-autorizaciones. [Accedido: 15-mar-2026].

[52] Aplirh, “Modelo de autorizaciones en SAP: de la gestión de roles…,” 2025. [En línea]. Disponible en: https://aplirh.es/asignacion-de-roles-a-usuarios-como-optimizar-tiempo-y-trazabilidad-en-sap/. [Accedido: 15-mar-2026].

[53] Novis, “Roles en SAP: cómo funcionan y cómo definirlos,” 2021. [En línea]. Disponible en: https://www.novis.com.mx/blog/sap/roles-y-perfiles-de-sap-como-funcionan-y-como-definirlos-12666/. [Accedido: 15-mar-2026].

[54] SAP, “Gestión de la seguridad mediante autorizaciones basadas en la función (SAP SuccessFactors Platform),” 2024. [En línea]. Disponible en:

(módulo Managing Security Using SAP SuccessFactors Platform en https://learning.sap.com). [Accedido: 15-mar-2026].

[55] Z-Net, “Tutorial: cómo filtrar sitios por categorías y listas negras en Fortigate,” s. f. [En línea]. Disponible en: https://www.z-net.com.ar/blog-post/9-tutorial-como-filtrar-sitios-por-categorias-y-listas-negras-en-fortigate/. [Accedido: 15-mar-2026].

[56] Fortinet, “Servicio de filtrado web FortiGuard,” s. f. [En línea]. Disponible en: https://www.fortinet.com/lat/support/support-services/fortiguard-security-subscriptions/web-filtering. [Accedido: 15-mar-2026].