República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Facultad de Posgrado e Investigación

Tesis en opción al título de Magíster en:

Ciberseguridad

Tema de Tesis:

Impacto Silencioso: Identidades Privilegiadas y Riesgos Emergentes en la Ciberseguridad de CORTRIP

Línea de Investigación:

Línea 4, Investigación, gestión del conocimiento, tecnologías de la informática y las comunicaciones.

Autor:

Ing. José Vicente Núñez Noboa

Director de Tesis:

Ing. Xavier Mosquera R., MSc.

Abril, 2024

Guayaquil – Ecuador

Yo José Vicente Núñez Noboa, con cédula de ciudadanía Nº 0914046081, autor de la presente tesis titulada *Impacto Silencioso: Identidades Privilegiadas y Riesgos Emergentes en la Ciberseguridad de CORTRIP*, mediante el presente dejo constancia que esta tesis es de mi exclusiva autoría y producción. El desarrollo de esta tesis tiene el objetivo de cumplir con un requisito previos a la obtención del título de Magíster en Ciberseguridad, de la Universidad Tecnológica Empresarial de Guayaquil por lo cual:

1. Autorizo a la Universidad Tecnológica Empresarial de Guayaquil, el derecho de publicar esta tesis, como artículo en publicaciones para lectura, fuentes de investigación, siempre dando a conocer el nombre del autor y respeto de la propiedad intelectual del mismo.

2. Declaro en caso de presentar cualquier reclamo por parte de terceros respecto de los derechos del autor de esta tesis antes mencionada yo asumiré toda responsabilidad frente a la universidad.

Guayaquil, Marzo del 2024.

AUTOR

José Vicente Núñez Noboa
C.C. 0914046081

DEDICATORIA:

A mi familia, por su amor incondicional, por su paciencia, comprensión, aliento apoyo y sacrificio a lo largo de este viaje académico, ustedes son mi motor y Dios mi gasolina. A mis amigos y seres queridos, por estar siempre presentes, brindándome fuerza y motivación. Este trabajo está dedicado a ustedes, quienes han sido mi luz en los momentos más oscuros.

AGRADECIMIENTO:

Agradezco sinceramente a todos los especialistas tanto de Cortrip como a los externos que participaron en este estudio, por su tiempo, cooperación y valiosas perspectivas que fueron fundamentales para comprender mejor los temas abordados en esta tesis.

Mi gratitud se extiende a mis compañeros de clase y colegas, por sus debates estimulantes, intercambio de ideas y solidaridad durante todo el proceso de investigación.

Finalmente, quiero expresar mi eterna gratitud a todas aquellas personas cuyo apoyo, ya sea grande o pequeño, ha sido fundamental en este camino hacia la culminación de este trabajo. Sus contribuciones han sido fundamentales para alcanzar este logro."

RESUMEN:

Este estudio sumerge a los lectores en la intrincada trama de las identidades privilegiadas en el contexto de las Tecnologías de la Información y Comunicación (TIC), específicamente dentro del entorno institucional de CORTRIP. A través de una exploración minuciosa, se analiza en detalle cómo las dinámicas de poder y las disparidades socioeconómicas desempeñan un papel crucial en la configuración de estas identidades privilegiadas. Se delinean sus impactos significativos en el acceso, uso y control de las TIC en entornos de Infraestructuras tecnológicas y de ciberseguridad de la Institución. Este examen de las dinámicas de poder también aborda los riesgos emergentes asociados. El estudio profundiza en cuestiones cruciales relacionadas con la seguridad, la privacidad y la equidad en el uso de las TIC, subrayando las complejidades inherentes a estas interacciones. Este análisis crítico no solo enriquece la comprensión de las implicaciones sociales y éticas de las identidades privilegiadas en el ámbito de las TIC, sino que también ofrece perspectivas valiosas. Estas perspectivas no solo son esenciales para comprender la complejidad de las interacciones en juego, sino que también sirven como guía para el diseño de políticas y buenas prácticas que fomenten la inclusión y la equidad en los entornos de Infraestructuras tecnológicas y de ciberseguridad de la Institución. En última instancia, se busca promover un enfoque más holístico y justo hacia la ciberseguridad en CORTRIP, contribuyendo así a la construcción de un entorno más seguro y equitativo en el uso y responsabilidad de los roles de identidades privilegiadas en la administración de las herramientas de tecnologías Institucionales.

PALABRAS CLAVES:

Identidades privilegiadas, Riesgos emergentes, Dinámicas de poder, Disparidades socioeconómicas, Seguridad Informática.

ABSTRACT:

This study immerses readers in the intricate web of privileged identities in the context of Information and Communication Technologies (ICT), specifically within the institutional environment of CORTRIP. Through close exploration, it examines in detail how power dynamics and socioeconomic disparities play a crucial role in shaping these privileged identities. Its significant impacts on the access, use and control of ICT in technological infrastructure and cybersecurity environments of the Institution are outlined. This examination of power dynamics also addresses the associated emerging risks. The study delves into crucial issues related to security, privacy and equity in the use of ICT, highlighting the complexities inherent in these interactions. This critical analysis not only enriches the understanding of the social and ethical implications of privileged identities in the ICT field, but also offers valuable insights. These perspectives are not only essential to understand the complexity of the interactions at play, but also serve as a guide for the design of policies and good practices that promote inclusion and equity in the Institution's technological infrastructure and cybersecurity environments. Ultimately, CORTRIP seeks to promote a more holistic and fair approach to cybersecurity, thus contributing to the construction of a more secure and equitable environment in the use and responsibility of the roles of privileged identities in the administration of technology tools. Institutional.

KEY WORDS:

Privileged identities, Emerging risks, Power dynamics, Socioeconomic disparities, Computer Security.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE CUADROS

INTRODUCCIÓN

En la contemporánea era digital, las Tecnologías de la Información y Comunicación (TIC) han emergido como catalizadores cruciales de transformación en los entornos institucionales. Esta investigación se sumerge en la intrincada red de las identidades privilegiadas en el ámbito de las TIC, explorando la compleja interacción entre estas identidades, las dinámicas de poder y los riesgos emergentes en contextos institucionales, bajo el título "Impacto Silencioso: Identidades Privilegiadas y Riesgos Emergentes en la Ciberseguridad de la Corporación de Tripulación De La Armada (CORTRIP)".

La vertiginosa evolución tecnológica ha introducido una nueva dimensión en la estructuración social, donde el acceso, la utilización y el control de las TIC se han convertido en determinantes clave de la posición e influencia dentro de CORTRIP. Más allá de meras discusiones sobre el acceso técnico, la desigualdad en el ámbito de las TIC trasciende la mera disponibilidad física de dispositivos y conexiones.

Esta investigación propone explorar las complejidades de las identidades privilegiadas, desde la posesión de habilidades digitales hasta la capacidad de influir en las decisiones tecnológicas en entornos institucionales. ¿Quiénes son los actores que ostentan estas identidades privilegiadas y cómo configuran estas interacciones en el espacio digital de CORTRIP?

La literatura actual indica que estas desigualdades no solo se limitan al acceso técnico según roles de privilegio, sino que también reflejan y refuerzan disparidades socioeconómicas preexistentes (CEPAL, 2020). A medida que las TIC se integran más profundamente en las operaciones diarias de las instituciones, la brecha se amplía entre aquellos que pueden aprovechar plenamente estas herramientas y aquellos que quedan marginados digitalmente. Este fenómeno plantea preguntas críticas sobre la equidad y la justicia en el panorama digital y cómo las instituciones pueden abordar efectivamente estas controversias.

El propósito de esta investigación es analizar no solo la distribución desigual de recursos tecnológicos, sino también las complejas interacciones de poder que

subyacen a la creación y perpetuación de identidades privilegiadas en entornos de TIC de CORTRIP. En este contexto, se busca comprender los riesgos emergentes asociados con estas dinámicas, como la seguridad informática, la privacidad en línea y la equidad digital, elementos esenciales para entender las implicaciones sociales y éticas de las identidades privilegiadas en el uso de las TIC en la actualidad.

La elección de un enfoque metodológico Delphi para esta investigación se justifica por su capacidad para recoger y analizar opiniones de expertos de manera iterativa, permitiendo la construcción de consensos y la exploración de perspectivas diversas. En el contexto específico de las complejas relaciones entre identidades privilegiadas en TIC y la ciberseguridad en CORTRIP, este método proporcionará una comprensión más holística y profunda.

En la era de la industria 4.0, las Tecnologías de la Información y Comunicación (TIC) han transformado radicalmente la forma en que las instituciones operan, pero la intersección entre identidades privilegiadas y ciberseguridad sigue siendo un terreno poco explorado. Este enfoque metodológico Delphi permitirá aunar la experiencia y la percepción de expertos en el campo, desentrañando las complejidades inherentes a estas dinámicas y ofreciendo una visión más completa de los desafíos y oportunidades que enfrenta CORTRIP en su entorno digital.

La metodología Delphi implicará la participación de un panel de expertos cuidadosamente seleccionados, quienes, a través de rondas sucesivas de cuestionamientos estructurados, proporcionarán sus opiniones y evaluaciones sobre las interacciones entre identidades privilegiadas y ciberseguridad en el contexto específico de CORTRIP. Este proceso iterativo permitirá refinar las respuestas a lo largo del tiempo, identificando patrones emergentes y áreas de acuerdo o desacuerdo entre los participantes.

Dada la complejidad de las relaciones en juego, el enfoque Delphi permitirá capturar la diversidad de perspectivas y experiencias de los expertos, superando posibles sesgos individuales y proporcionando una representación más completa de la realidad en CORTRIP. Además, la iteración continua del proceso permitirá

adaptarse a medida que surjan nuevas percepciones o se desarrollen dinámicas inesperadas en el ámbito de las identidades privilegiadas y la ciberseguridad.

Al adoptar este enfoque, se busca no solo profundizar en la comprensión de los problemas identificados, sino también generar conocimientos que puedan informar directamente las prácticas y políticas en CORTRIP. La aplicabilidad y relevancia de los resultados se maximizarán al integrar la experiencia de aquellos que están directamente involucrados en el ámbito de estudio, contribuyendo así a un marco más sólido y aplicable para abordar los desafíos de las identidades privilegiadas en el contexto de la ciberseguridad.

Contextualización e importancia del tema

La creciente interconexión de la sociedad contemporánea con las Tecnologías de la Información y Comunicación (TIC) ha generado un entorno en constante evolución en el que las identidades privilegiadas desempeñan un papel crucial. En particular, la Corporación de Tripulación de La Armada (CORTRIP) se encuentra inmersa en un contexto digital donde las dinámicas de poder y las implicaciones en ciberseguridad relacionadas con estas identidades han recibido escasa atención. Este estudio surge en un momento crítico, en la era de la industria 4.0, donde las instituciones a nivel mundial se ven confrontadas con desafíos complejos relacionados con las TIC y las identidades privilegiadas, desafíos cuyas ramificaciones en el ámbito de la ciberseguridad han permanecido en gran parte inexploradas.

Propósito general de la investigación

El propósito fundamental de esta investigación es explorar, mediante un enfoque metodológico Delphi, las intrincadas relaciones entre las identidades privilegiadas en el uso de las TIC y los aspectos asociados a la ciberseguridad en CORTRIP. Al ofrecer un análisis profundo y perspicaz, se busca contribuir de manera significativa al cuerpo de conocimientos en este campo crítico, arrojando luz sobre las complejidades que rodean estas temáticas y proporcionando ***insights*** (descubrimientos o revelaciones que pueden ayudar a las empresas valiosas) para abordar los desafíos emergentes en el entorno digital de la Corporación.

Breve descripción de los apartados que componen el trabajo

Capítulo I. Marco Teórico Conceptual: Este capítulo se centra en establecer los fundamentos teóricos y conceptuales que respaldan la investigación. Se explorarán las teorías relevantes sobre identidades privilegiadas en el contexto de las TIC, las dinámicas de poder, y se proporcionará una revisión exhaustiva de la literatura existente que sustenta la investigación.

Capítulo II. Marco Metodológico: En este apartado se detallará el enfoque metodológico Delphi seleccionado para llevar a cabo la investigación. Se explicarán los procedimientos, las fases y las técnicas empleadas para recopilar y analizar la información, así como las razones detrás de la elección de este enfoque específico.

Capítulo III. Resultados y Discusión: Este capítulo presentará los hallazgos obtenidos a través del análisis Delphi. Se discutirán las complejas relaciones identificadas entre las identidades privilegiadas en TIC y los aspectos de ciberseguridad en CORTRIP, analizando los resultados en función de las teorías revisadas en el Marco Teórico Conceptual.

Capítulo IV. Propuesta: En la última sección, se formularán propuestas basadas en los resultados y la discusión previa. Estas sugerencias podrían incluir recomendaciones para políticas internas, prácticas de seguridad, y estrategias para fomentar la equidad y la seguridad en el uso de las TIC en CORTRIP.

En conjunto, estos capítulos pretenden proporcionar una visión integral y estructurada de la investigación, desde su fundamento teórico hasta las propuestas concretas para abordar los desafíos identificados, contribuyendo así al avance del conocimiento en este ámbito esencial.

CAPÍTULO I.

MARCO TEÓRICO CONCEPTUAL

En este capítulo, se exponen los antecedentes relacionados con temáticas similares abordadas en el ámbito de las *Identidades Privilegiadas* en sistemas de gestión de seguridad informática. Asimismo, se proporcionan las bases teóricas esenciales para el desarrollo del tema de investigación. Por último, se procede a definir los términos más relevantes que serán considerados a lo largo de todo el proyecto.

1.1 Antecedentes de la investigación

Los antecedentes que se describen a continuación constituyen investigaciones en diversas Universidades. Estas investigaciones han abordado temáticas afines a los objetivos planteados en el presente caso de estudio.

A continuación, se describen diferentes puntos de varios casos de estudios como antecedentes:

Alruwies M. (2021), *"Identity Governance Framework for Privileged Users"*; el artículo aborda la creciente complejidad en la gestión de identidades y accesos en el ámbito de la tecnología de la información (TI). Destaca la necesidad de proteger activos valiosos en empresas de TI, donde cada aplicación tiene su propio mecanismo de autenticación y los empleados deben lidiar con múltiples nombres de usuario y contraseñas. El aumento en el número de solicitudes ha complicado la administración de identidades y derechos de acceso asociados.

Título:

"Identity Governance Framework for Privileged Users"

Problemática Identificada:

La problemática identificada en el estudio "Identity Governance Framework for Privileged Users" de Alruwies (2021) se centra en la creciente complejidad en la gestión de identidades y accesos en el ámbito de la tecnología de la información (TI). A continuación, se detallan algunas de las problemáticas identificadas:

- Complejidad en la gestión de identidades y accesos: El aumento en el número de solicitudes y la presencia de múltiples nombres de usuario y contraseñas generan una complejidad significativa en la administración de identidades y derechos de acceso en entornos de TI.

- Diversidad de mecanismos de autenticación y autorización: Cada aplicación en el entorno de TI tiene su propio mecanismo de autenticación y autorización, lo que complica aún más la gestión de identidades y accesos. La falta de estandarización puede llevar a dificultades en la administración y coordinación eficientes.

- Desafíos en la protección de activos valiosos: La necesidad de proteger activos valiosos en empresas de TI se ve comprometida debido a la complejidad y la diversidad de los mecanismos de seguridad en las aplicaciones individuales.

- Problemas asociados con usuarios privilegiados: La gestión de usuarios privilegiados presenta desafíos adicionales, ya que estos usuarios tienen acceso a información crítica y, por lo tanto, requieren una atención especial en términos de control y supervisión.

- Ineficiencia en la gestión descentralizada: La gestión descentralizada de identidades y accesos, con múltiples aplicaciones manejando sus propios mecanismos, se percibe como ineficiente y propensa a fallos.

El artículo propone abordar estas problemáticas mediante la introducción de un marco de gobernanza y gestión de identidad, centrándose especialmente en la gestión de acceso privilegiado. La propuesta incluye la centralización de la gestión de identidades y accesos, con un enfoque híbrido que integra la gestión de identidades y el acceso privilegiado utilizando Active Directory. Se argumenta que esta integración contribuirá a la eficiencia en la administración de derechos de acceso y mejorará la capacidad de respuesta a desafíos de ciberseguridad, con especial énfasis en el contexto de la digitalización acelerada debido a la pandemia de COVID-19.

Objetivos del Proyecto:

En base a la descripción del estudio "Identity Governance Framework for Privileged Users" de Alruwies (2021), los objetivos del proyecto son los siguientes:

- Desarrollar un Marco de Gobernanza de Identidad: Diseñar y establecer un marco integral de gobernanza para la gestión de identidades en entornos de tecnología de la información, con un enfoque específico en la administración de accesos privilegiados.

- Centralizar la Gestión de Identidades y Accesos: Implementar un sistema que centralice la gestión de identidades y derechos de acceso, buscando superar la complejidad asociada con la diversidad de mecanismos de autenticación y autorización en diversas aplicaciones.

- Optimizar la Eficiencia en la Administración de Derechos de Acceso: Mejorar la eficiencia en la administración de derechos de acceso, especialmente para usuarios privilegiados, mediante la integración de un enfoque híbrido que utilice Active Directory.

- Mejorar la Seguridad de la Información: Fortalecer la seguridad de la información mediante la implementación de prácticas y controles que minimicen los riesgos asociados con la gestión descentralizada de identidades y accesos.

- Facilitar la Respuesta a Incidentes de Seguridad: Desarrollar capacidades que permitan a las organizaciones responder eficientemente a incidentes de seguridad, asegurando la capacidad de identificar y abordar amenazas en tiempo real.

- Cumplir con los Requisitos de Seguridad y Normativas: Asegurar que el marco propuesto cumple con los requisitos de seguridad establecidos por normativas y estándares relevantes, garantizando así la conformidad con regulaciones específicas del sector.

- Integrar la Gestión de Identidades y Acceso Privilegiado con Active Directory:
  Implementar la integración propuesta con Active Directory para gestionar de manera eficiente la identidad y el acceso privilegiado, aprovechando las capacidades de esta herramienta.

- Adaptarse al Contexto de Digitalización Acelerada: Diseñar el marco de gobernanza de identidad considerando las demandas y desafíos específicos derivados de la digitalización acelerada, en particular, en respuesta a la pandemia de COVID-19.

Estos objetivos buscan abordar las problemáticas identificadas en el estudio y establecer un enfoque más eficiente y seguro para la gestión de identidades y accesos en el ámbito de la tecnología de la información.

Para abordar estos desafíos, los autores proponen un marco de gobernanza y gestión de identidad para infraestructuras de información y tecnología con gestión de acceso privilegiado. Este enfoque busca centralizar la gestión de identidades y accesos, especialmente para usuarios privilegiados, en lugar de depender de múltiples aplicaciones con sus propios mecanismos de autenticación y autorización.

Se destaca la eficiencia de este marco en comparación con los componentes de seguridad de la información existentes. Además, se aborda la importancia de la gestión integrada de identidad y acceso para permitir a las organizaciones responder a incidentes y cumplir con requisitos de seguridad, especialmente en el contexto de la digitalización acelerada debido a la pandemia de COVID-19.

El artículo propone un enfoque híbrido que integra la gestión de identidades y el acceso privilegiado utilizando Active Directory. Se argumenta que esta integración facilita la administración de derechos de acceso y la respuesta a desafíos de ciberseguridad.

Conclusión:

El artículo aborda la complejidad en la gestión de identidades y accesos en empresas de TI, proponiendo un marco de gobernanza y gestión de identidad para abordar estos problemas. Además, destaca la importancia de la gestión integrada de identidad y acceso, especialmente en el contexto actual de aumento de la digitalización y trabajo en línea.

Contreras (2019)*" Implementación De Un Sistema De Gestión De Identidades Privilegiadas Para El Control De Acceso En Una Empresa De RETAIL"*, en este proyecto se describe la implementación de un Sistema de Gestión de Acceso Privilegiado en una empresa de RETAIL con el objetivo de mejorar la gestión de identidades privilegiadas de los administradores de las plataformas de Tecnologías de la Información (TI).

Título:

Implementación De Un Sistema De Gestión De Identidades Privilegiadas Para El Control De Acceso En Una Empresa De RETAIL

Problemática Identificada:

- Ineficiencia en la gestión de identidades privilegiadas de los administradores de las plataformas de TI en la empresa de RETAIL.
- Lentitud en el proceso de autenticación.
- Riesgo potencial de extracción de información por usuarios no autorizados.
- Demoras significativas en los procesos de aprobación de acceso a dispositivos críticos y en el control de cambios durante la fase de producción.

Objetivos del Proyecto:

- Agilizar el proceso de autenticación en los activos de TI para aumentar la eficiencia operacional.
- Mitigar el riesgo de extracción de información por usuarios no autorizados.
- Reducir el tiempo necesario para el proceso de aprobación de acceso a dispositivos críticos en la fase de producción de la empresa.

Propósito Principal:

Optimizar la gestión de identidades privilegiadas para mejorar la eficiencia operativa y mitigar amenazas a la seguridad de la información.

Enfoque del Proyecto:

- Implementación de un Sistema de Gestión de Acceso Privilegiado.
- Establecimiento de políticas para prevenir LEAPFROG (posible referencia a algún tipo de amenaza).
- Control exhaustivo y registro detallado de las actividades de los usuarios.
- Proporcionar trazabilidad de los cambios realizados en los activos de TI.

Metodología:

- Utilización del método Plan-Do-Check-Act (PDCA), recomendado por la norma ISO/IEC 27001:2013.
- Aplicación de controles específicos relacionados con la gestión de credenciales para garantizar la protección integral de la información.

Resultados de la Implementación:

- Minimización efectiva de los riesgos asociados a amenazas y vulnerabilidades sobre los activos críticos de TI de la empresa de RETAIL.
- Mejora en aspectos clave como la confidencialidad, disponibilidad e integridad de la información.

Conclusión:

El proyecto se centra en mejorar la seguridad y eficiencia en la gestión de identidades privilegiadas en una empresa de RETAIL mediante la implementación de un Sistema de Gestión de Acceso Privilegiado. La metodología utilizada sigue las mejores prácticas establecidas por la norma ISO/IEC 27001:2013.

Carmona (2023)*, "Modelo de monitoreo para la detección de escenarios de riesgo asociados a la identidad y control de acceso mediante la integración de*

una solución IAM con un SIEM para mejorar la respuesta a incidentes de seguridad".

Contexto:

- Destaca la creciente importancia de la identidad en el contexto digital actual.
- Aborda la problemática de la sobrecarga de alertas para los equipos de seguridad y la necesidad de agilizar los procesos de respuesta a incidentes.

A continuación, se describen los diferentes puntos del caso de estudio:

Título:

Modelo de monitoreo para la detección de escenarios de riesgo asociados a la identidad y control de acceso mediante la integración de una solución administración de identidad y acceso (IAM) con La Administración de eventos e información de seguridad, (SIEM), para mejorar la respuesta a incidentes de seguridad.

Descripción:

El estudio del caso se enfoca en mejorar la respuesta a incidentes de seguridad mediante la integración de soluciones de gestión de identidades (IAM) con un Sistema de Información y Eventos de Seguridad (SIEM). El objetivo principal es obtener evidencias de ataques en forma de alertas que se reportarán en el tablero de control del SIEM.

Metodología:

Definición de Herramientas:

- Inicio con la definición de herramientas necesarias y la implementación de software complementario.
- Se seleccionaron soluciones Opensource para el proyecto.

Integración de Soluciones:

- Implementación de soluciones IAM y SIEM seleccionadas.
- Se buscó la viabilidad de la integración IAM-SIEM y la ausencia de limitaciones en la versión gratuita.

Evaluación de Soluciones SIEM:

- Se evaluaron varias soluciones SIEM Opensource (AlientVault OSSIM, Apache Metron, Mozdef, Wazuh).
- Se descartaron AlientVault OSSIM y Apache Metron por limitaciones y retiro del proyecto.
- Mozdef fue eliminado por falta de mantenimiento.
- Se seleccionó Wazuh como la solución final debido a sus capacidades integrales de detección de intrusos y configurabilidad.

Propuesta de Modelo de Monitoreo:

- Enfocado en la integración de una solución IAM y un SIEM de código abierto.
- Asignación de puntajes de riesgo para descartar alertas basadas en configuraciones y políticas para cada cuenta.
- Focalización en amenazas genuinas para agilizar la respuesta a incidentes.

Validación del Modelo:

- Validación mediante ataques controlados.
- Demostración de una mejora significativa en los tiempos de respuesta a incidentes de seguridad.
- Proporciona una lista más reducida de alertas pertinentes.

Conclusión:

El estudio propone un modelo de monitoreo integral que integra IAM y SIEM para mejorar la detección y respuesta a incidentes de seguridad, demostrando su

eficacia mediante la validación con ataques controlados. Wazuh se elige la solución SIEM final debido a sus capacidades y flexibilidad.

Cascales (2020)*, "Informe De Asesoramiento Basado En La Arquitectura De Referencia De Ciberseguridad De Microsoft Para La Empresa Veiligheidsregio Twente",* este informe de asesoramiento se basa en la arquitectura de referencia de ciberseguridad de Microsoft para la empresa Veiligheidsregio Twente (VRT).

A continuación, se describen los diferentes puntos del caso de estudio:

Titulo:

Informe De Asesoramiento Basado En La Arquitectura De Referencia De Ciberseguridad De Microsoft Para La Empresa Veiligheidsregio Twente.

Contexto:

- El informe se centra en proporcionar asesoramiento basado en la arquitectura de referencia de ciberseguridad de Microsoft.
- El cliente, VRT, expresó satisfacción general con la utilidad y practicidad de la investigación y los consejos proporcionados.

Resultados del Proyecto:

- El proyecto se considera implementable y orientado a la acción, diferenciándose de otros proyectos.
- Se logra el objetivo de proporcionar asesoramiento para la implementación de Azure AD y AIP conforme a las mejores prácticas y normas de seguridad.

Acciones Por Realizar:

- Se abordó la falta de una lista resumen de acciones mediante la creación de dicha lista, adjuntándola como un apéndice al documento.

Asesoramiento y Mejoras Propuestas:

- Se incluyen recomendaciones para mejorar la seguridad del entorno, abarcando aspectos como la supervisión, PAM, IAM para Azure AD, etiquetado unificado para Azure Information Protection, entre otros.
- Prácticas recomendadas incluyen la evaluación periódica y registro de cuentas de administrador, la monitorización activa de eventos de Active Directory, la limpieza regular de cuentas antiguas, y más.

Resultados Positivos y Logro de Objetivos:

- Se cumplen todos los requisitos establecidos con el cliente.
- Se insta a VRT a implementar las recomendaciones para Azure AD y AIP utilizando el resumen proporcionado en el apéndice como guía.

Importancia del Proyecto:

- Fundamental para comprender las tecnologías de ciberseguridad de Microsoft y su integración con arquitecturas existentes.
- La implementación de los cambios en el sistema se lleva a cabo de manera exitosa, demostrando beneficios para ambas partes.

Satisfacción del Cliente:

VRT está satisfecha con el informe de asesoramiento y planea ponerlo en práctica con la asistencia del servicio técnico de Microsoft debido a la naturaleza confidencial de los datos.

Conclusión:

El proyecto se considera un éxito, logrando sus objetivos y proporcionando recomendaciones prácticas para mejorar la seguridad del entorno de VRT, con una respuesta positiva y satisfacción continua por parte del cliente.

1.2 Planteamiento del problema de investigación

El planteamiento de este problema radica en la falta de conciencia y comprensión adecuadas en las instituciones públicas y privadas en referencia como caso de estudio delimitado al CORTRIP sobre la magnitud de los riesgos asociados con las identidades privilegiadas en el entorno de las TIC. La carencia de una gestión

efectiva de estas identidades puede conducir a brechas de seguridad, fugas de datos y potenciales amenazas tanto internas como externas. Además, el impacto de los riesgos de identidades privilegiadas en la integridad, confidencialidad y disponibilidad de la información institucional es una preocupación crítica.

Por lo tanto, se plantea la necesidad de investigar y comprender a fondo el *“Impacto Silencioso de Identidades Privilegiadas y los Riesgos Emergentes de CORTRIP”*. Esta investigación tiene como objetivo identificar y evaluar los desafíos específicos que enfrentan la institución en la gestión de identidades privilegiadas y proponer estrategias efectivas para mitigar estos riesgos, así como fortalecer la seguridad en el ámbito de las TIC.

1.2.1 Formulación del Problema

En la actualidad, el panorama de rápida evolución tecnológica y la cada vez mayor integración de las Tecnologías de la Información y Comunicación (TIC) en entornos institucionales plantean un desafío fundamental, en el *"Impacto Silencioso: Identidades Privilegiadas y Riesgos Emergentes en la Ciberseguridad de CORTRIP"*. Este problema se manifiesta de manera destacada en la configuración de identidades privilegiadas que afectan el acceso, uso y control de las TIC dentro de CORTRIP, dando lugar a riesgos emergentes en el ámbito de la ciberseguridad. La necesidad crítica de abordar este fenómeno requiere una formulación precisa y contextualizada para comprender sus complejidades y consecuencias en el entorno institucional de CORTRIP.

Pregunta de Investigación:

- *¿Cómo afectan las identidades privilegiadas y los riesgos emergentes en la ciberseguridad de Cortrip, y cuáles son las implicaciones para la protección de la información y la infraestructura digital?*

1.2.2 Sistematización del Problema

La sistematización del problema, es esencial en este caso de estudio resulta crucial para establecer una estructura clara y organizada que facilite la comprensión y abordaje de las complejidades asociadas con las identidades privilegiadas en el uso de Tecnologías de la Información y Comunicación (TIC) y los riesgos emergentes en entornos institucionales.

Dimensión de Identidades Privilegiadas:

La Dimensión de Identidades Privilegiadas, en el contexto de esta investigación, plantea la necesidad de explorar la distribución del acceso físico y las disparidades en la disponibilidad de dispositivos y conexiones en entornos de ciberseguridad asociados a CORTRIP.

- ¿Cómo contribuyen estas condiciones a la configuración de identidades privilegiadas en el uso de TIC dentro de CORTRIP? Asimismo, se plantea la interrogante sobre el impacto de las habilidades digitales, la participación y la productividad dentro de la institución.

- *¿Quiénes tienen acceso a oportunidades de desarrollo de estas habilidades, y cómo esto influye en la configuración y perpetuación de identidades privilegiadas en el uso y control de las TIC?*

Además, se busca comprender de qué manera las dinámicas de poder en las estructuras organizativas, la toma de decisiones tecnológicas y la influencia en políticas tecnológicas contribuyen a la creación y mantenimiento de identidades privilegiadas.

- *¿Cuáles son los riesgos tecnológicos emergentes asociados a estas configuraciones en entornos institucionales?*

Estas preguntas específicas orientan la investigación hacia una comprensión más profunda de las complejidades subyacentes a las identidades privilegiadas y sus impactos en la ciberseguridad de la institución CORTRIP.

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Analizar el impacto de las identidades privilegiadas y los riesgos emergentes en el sistema de ciberseguridad de Cortrip.

1.3.2 Objetivos Específicos

Con el enfoque de este caso de estudio, se delinean los siguientes objetivos específicos, siguiendo las reglas establecidas para la declaración de objetivos:

- *Realizar un análisis exhaustivo de los riesgos particulares relacionados con las identidades privilegiadas en el contexto de las (TIC), identificando amenazas potenciales y vulnerabilidades clave.*

- *Proponer mejores prácticas en el manejo de identidades privilegiadas en el ámbito de las TIC, con el objetivo de identificar las más eficaces y adecuadas para abordar los riesgos identificados.*

- *Elaborar recomendaciones concretas y estrategias efectivas para fortalecer la seguridad de las identidades privilegiadas en las TIC, con un enfoque en la mitigación de riesgos y la protección de los activos de la organización.*

1.4 Justificación de la investigación

La imperante necesidad de abordar los riesgos potenciales y entender el *"Impacto Silencioso de Identidades Privilegiadas y los Riesgos Emergentes de CORTRIP"* motiva esta investigación. A pesar de la trascendental importancia de estas identidades en la infraestructura tecnológica de la institución, se percibe una falta generalizada de conciencia acerca de los riesgos asociados a prácticas de gestión inadecuadas en muchas organizaciones por la falta de presupuestos o la creencia de que invertir en seguridad informática es una pérdida de dinero y tiempo.

Esta investigación se proyecta como un aporte significativo al ayudar a las instituciones a resguardar sus activos críticos y a mantener la confianza de sus ***stakeholders*** *(es el público de interés para una empresa que permite su completo funcionamiento. Es decir, a todas las personas u organizaciones que se relacionan con las actividades y decisiones de una empresa como: empleados, proveedores, clientes, gobierno, entre otros)* en un entorno digital en constante evolución. Asimismo, proporciona una base sólida para decisiones informadas en la gestión de identidades privilegiadas en el contexto de las TIC.

La comprensión de las identidades privilegiadas en el uso de las TIC y los riesgos asociados en entornos institucionales se considera esencial por varias razones cruciales:

- Equidad y Justicia Social: Identificar y comprender las identidades privilegiadas posibilita abordar las desigualdades tecnológicas, trabajando hacia una distribución más equitativa de recursos y oportunidades.

- Toma de Decisiones Informada: La identificación de riesgos tecnológicos emergentes asociados con identidades privilegiadas proporciona información vital para decisiones informadas en la implementación y gestión de TIC en entornos institucionales.

- Diseño de Políticas y Prácticas: Comprender las dinámicas de poder y los riesgos tecnológicos contribuye al diseño de políticas y prácticas institucionales que fomentan la inclusión digital y la equidad en el acceso y uso de las TIC.

- Desarrollo de Estrategias de Mitigación: Identificar los problemas inherentes a las identidades privilegiadas en TIC permite desarrollar estrategias de mitigación efectivas para abordar los riesgos y promover un entorno tecnológico más seguro y equitativo.

- Impacto Potencial: Este estudio busca no solo describir el problema de las identidades privilegiadas en TIC y los riesgos emergentes en entornos de ciberseguridad, sino también proporcionar información valiosa para la acción práctica.

Los resultados de esta investigación tienen el potencial de influir en la formulación de políticas, guiar la implementación de tecnologías de manera ética y promover la equidad digital en diversos ámbitos institucionales, desde la educación hasta el sector empresarial. La resolución efectiva de este problema contribuirá a construir entornos tecnológicos más inclusivos, justos y seguros en la era digital actual.

1.5 Marco de referencia de la investigación

El presente estudio se inscribe en un contexto de creciente interdependencia entre las instituciones y las Tecnologías de la Información y Comunicación (TIC),

suscitando una conciencia cada vez mayor sobre los riesgos asociados con la gestión de identidades privilegiadas en estos entornos. El marco de referencia se apoya en diversas áreas claves de conocimiento y teoría directamente relacionadas con los objetivos de esta investigación.

Identidades Privilegiadas.

Las "Identidades Privilegiadas" se refieren a cuentas, roles o usuarios en un sistema informático que tienen niveles de acceso y permisos más elevados que los usuarios normales. Estas identidades suelen tener privilegios especiales que les otorgan la capacidad de realizar acciones críticas o sensibles en un sistema, (IBM, 2024)

En el ámbito de la ciberseguridad, las identidades privilegiadas.

Pueden incluir, por ejemplo, cuentas de administradores de sistemas, Super Usuarios, o cualquier cuenta que tenga acceso a información confidencial o funciones críticas en una red. Dado que estas cuentas tienen mayores privilegios, su compromiso o mal uso puede representar un riesgo significativo para la seguridad de la información, (IBM, 2024)

El manejo adecuado de las identidades privilegiadas.

Es crucial para la seguridad cibernética, ya que su compromiso podría llevar a la exposición de datos sensibles, manipulación no autorizada de sistemas o incluso la interrupción de operaciones críticas, (Microsoft, 2024)

Seguridad Informática.

Este apartado aborda las teorías y prácticas relacionadas con la gestión de identidades privilegiadas y su impacto en la seguridad informática. Se consideran teorías y modelos de seguridad de la información, como el Modelo de Triángulo de Seguridad y el Ciclo de Vida de Identidades Privilegiadas, (Cisco, 2024)

Gestión de Riesgos en TIC.

Explora la literatura y teoría relacionada con la gestión de riesgos en el contexto de las TIC, incluyendo el marco de gestión de riesgos ISO 31000. Esto permite comprender la importancia de identificar, evaluar y mitigar los riesgos en identidades privilegiadas, (ISO, 2024)

Mejores Prácticas en Gestión de Identidades Privilegiadas.

Se basa en investigaciones sobre las mejores prácticas en la gestión de identidades privilegiadas, incluyendo el principio de menor privilegio y estrategias de control de acceso. También se considera la literatura relacionada con soluciones tecnológicas como PAM (Privileged Access Management), (Microsoft, 2024)

Ciberseguridad Interna Threats.

Analiza los indicadores de compromiso relacionado con la ciberseguridad y las correlaciona con las amenazas internas de la institución, ya que las identidades privilegiadas pueden ser un objetivo para actores maliciosos dentro de la organización, (IBM, 2024)

Psicología del Insider Threat.

Se refiere a la investigación de la psicología de la amenaza interna. En el ámbito de la ciberseguridad, un "insider threat" (amenaza interna) se produce cuando individuos dentro de una organización utilizan su acceso privilegiado para comprometer la seguridad de la información. La investigación en la psicología de esta amenaza puede implicar entender las motivaciones, comportamientos y factores psicológicos que pueden llevar a un empleado a convertirse en una amenaza para la seguridad de la organización, (Ahmad, 2021).

Modelos de Detección Temprana.

Esto se refiere a la investigación de modelos o enfoques para detectar tempranamente posibles amenazas internas. La detección temprana es fundamental para prevenir o mitigar daños causados por insiders que podrían intentar realizar acciones maliciosas. Los modelos de detección temprana podrían involucrar algoritmos, análisis de comportamiento, o cualquier otro enfoque que permita identificar patrones de actividad sospechosa antes de que se produzcan eventos perjudiciales, (IBM, 2024)

1.5.1 Marco Normativo y Regulatorio.

Este apartado incluye una revisión de regulaciones y estándares relacionados con la seguridad informática, como GDPR, HIPAA y NIST, que establecen directrices específicas para la gestión de identidades privilegiadas. Se utilizará

el marco NIST SP 800-53 (2021) como guía para analizar los riesgos y proponer estrategias efectivas de mitigación en el ámbito de la investigación.

1.5.2 Marco Teórico.

El marco teórico proporciona las bases conceptuales que sustentan la comprensión profunda de las identidades privilegiadas en el uso de Tecnologías de la Información y Comunicación (TIC) y el *"Impacto Silencioso de Identidades Privilegiadas y los Riesgos Emergentes de CORTRIP"*. Este marco se apoya en diversas teorías que abordan aspectos clave de las dinámicas tecnológicas, sociales y éticas presentes en este contexto.

Teoría de las Desigualdades Tecnológicas.

Examina las disparidades en el acceso y uso de las TIC, considerando dimensiones como la infraestructura tecnológica, las habilidades digitales y la disponibilidad de recursos. En el contexto institucional, se explora cómo estas desigualdades contribuyen a la formación de identidades privilegiadas, (Clacso, 2019)

Teoría de la Brecha Digital.

Enfocándose en las brechas en acceso, uso y beneficios derivados de las TIC, esta teoría ayuda a entender cómo las diferencias socioeconómicas y culturales influyen en la configuración de identidades privilegiadas y en la exacerbación de riesgos tecnológicos en entornos institucionales, (Almenara, 2023)

Teoría de las Identidades Privilegiadas.

Se centra en las relaciones de poder que determinan quiénes tienen acceso preferencial a las TIC y cómo estas identidades privilegiadas se construyen y mantienen. Se analiza cómo estas dinámicas de poder afectan la toma de decisiones y el control tecnológico en CORTRIP, (McCarthy, 2023)

Teoría de Riesgos Tecnológicos Emergentes.

Examina los riesgos asociados con la implementación y uso de tecnologías emergentes. En el entorno de la Institución, se considera cómo las identidades privilegiadas pueden contribuir a la vulnerabilidad frente a amenazas de seguridad, pérdida de privacidad y desigualdades en la adopción de nuevas tecnologías, (Bejarano, 2023)

Teoría Ética de la Tecnología.

Desde una perspectiva ética, aborda las decisiones relacionadas con el diseño, implementación y uso de las TIC en la Institución. Se considera cómo las identidades privilegiadas pueden dar lugar a dilemas éticos y se exploran estrategias para abordar estos desafíos desde una perspectiva ética, (Queraltó, 2023)

Teoría Institucional.

Analiza cómo la institución como entidad social influye en la configuración de identidades privilegiadas en el ámbito tecnológico. Se exploran la estructura organizativa, la cultura institucional y las políticas que impactan en la adopción y gestión de las TIC, (Restrepo M., 2002).

Al integrar estas teorías, se construye un marco teórico sólido que proporciona un enfoque holístico para comprender las complejas interacciones entre identidades privilegiadas, riesgos tecnológicos y contextos de la institución, (Restrepo M., 2002).

1.5.3 Marco Contextual.

El marco contextual proporciona el entorno en el que se desarrolla la investigación, considerando elementos sociales, económicos y culturales que influyen en las dinámicas de identidades privilegiadas y riesgos tecnológicos en el entorno institucional. Para comprender completamente la relación entre estos factores y la implementación de Tecnologías de la Información y Comunicación (TIC), se abordan diferentes dimensiones dentro del contexto institucional.

Infraestructura Tecnológica.

Se examina la infraestructura tecnológica existente en la institución, incluyendo la disponibilidad de hardware, software y redes de datos. La calidad y accesibilidad de esta infraestructura tecnológica pueden afectar la equidad en el acceso y uso de las TIC, (IBM, 2023).

Prácticas Organizativas.

Las prácticas internas, protocolos y cultura organizativa impactan en la implementación y uso de las TIC. Se exploran las estructuras de toma de

decisiones, la flexibilidad organizativa y la adopción de nuevas tecnologías Díaz-Cabrera (2024).

Características Demográficas de los Usuarios: Las características demográficas de los usuarios, como edad, género, nivel educativo y roles institucionales, influyen en cómo las personas interactúan con las TIC, (Hill, 2023).

15.4 Marco legal.

El marco legal establece las normativas, regulaciones y políticas que rigen el uso de Tecnologías de la Información y Comunicación (TIC) en entornos institucionales en Ecuador. Este marco proporciona las directrices legales que estructuran la implementación, gestión y seguridad de las TIC, asegurando el cumplimiento de obligaciones y protegiendo los derechos fundamentales de los individuos. Al abordar estas dimensiones, se logra una comprensión integral de las limitaciones y obligaciones legales en las que operan las instituciones en el ámbito tecnológico.

Constitución de la República del Ecuador (2008).

La Constitución establece principios fundamentales relacionados con los derechos y garantías de las personas, incluyendo derechos relacionados con la privacidad y la protección de datos. Proporciona el marco ético y legal que guía el uso de las TIC en consonancia con los derechos fundamentales de los ciudadanos.

Ley Orgánica de Telecomunicaciones (LOT) y Reglamento General a la LOT.

La LOT regula el sector de las telecomunicaciones en Ecuador, abordando temas como la regulación de servicios de telecomunicaciones, el acceso a la información, derechos y obligaciones de los usuarios, y medidas de seguridad para las redes y servicios. El Reglamento General detalla disposiciones específicas para garantizar la seguridad y privacidad en las comunicaciones electrónicas.

Ley Orgánica de Comunicación (LOC).

La LOC regula el ámbito de la comunicación en Ecuador, incluyendo aspectos relacionados con medios de comunicación, publicidad y derechos de autor.

Establece parámetros legales para la difusión de información a través de las TIC, garantizando el respeto a la propiedad intelectual y la veracidad de la información.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
Esta ley establece el marco legal para el comercio electrónico en Ecuador, regulando la validez de contratos electrónicos, el uso de firmas electrónicas y la protección de la información contenida en mensajes de datos. Asegura la validez jurídica de las transacciones realizadas mediante TIC.

Ley Orgánica de Datos Personales (LOPD).
Esta ley regula el tratamiento de datos personales en Ecuador, estableciendo principios para la protección de la privacidad y los derechos de las personas sobre sus datos personales. Garantiza la adecuada gestión y seguridad de la información personal en entornos institucionales.

Ley Orgánica de Educación Superior (LOES).
Aunque no específica para TIC, la LOES puede ser relevante en el contexto institucional, especialmente en el ámbito educativo. Regula la educación superior en Ecuador, proporcionando directrices sobre la integración de TIC en procesos educativos.

Normativas y Regulaciones de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).
La ARCOTEL emite regulaciones específicas para el sector de las telecomunicaciones, abordando temas como la seguridad de la información, el acceso a servicios de telecomunicaciones, entre otros. Estas regulaciones complementan la LOT y aseguran la integridad de las comunicaciones electrónicas.

Leyes Penales y de Delitos Informáticos: Disposiciones en el Código Orgánico Integral Penal (COIP) relacionadas con delitos informáticos y la seguridad de la información. Establece consecuencias legales para acciones que comprometan la integridad y seguridad de sistemas informáticos.

Leyes de Propiedad Intelectual.

Ecuador tiene leyes que protegen la propiedad intelectual, incluyendo derechos de autor y patentes, que son relevantes para el ámbito digital. Estas leyes salvaguardan los derechos de los creadores y promueven la innovación en el uso de TIC.

Es crucial revisar las leyes y regulaciones específicas según el contexto y las necesidades particulares de la institución. El asesoramiento legal especializado puede ser necesario para garantizar el cumplimiento y la comprensión completa de las obligaciones legales en el uso de TIC en Ecuador.

CAPÍTULO II.

MARCO METODOLÓGICO

2.1 Métodos de investigación.

La presente investigación se centra en la exploración de *"Identidades Privilegiadas y Desafíos Emergentes en la Ciberseguridad de CORTRIP".*

El CORTRIP *(Corporación de Tripulación de la Armada)*. tiene como objetivo, Constituirse en una Corporación organizada que brinde excelentes servicios como hotelería, restaurante, eventos sociales, culturales y deportivos con personal calificado, comprometido con la buena atención y satisfacción para sus socios, dependientes y de la colectividad en general de las sedes que poseen actualmente en las ciudades de: Guayaquil, Quito, Manta. Salinas, Milagros y Esmeraldas actualmente y así proyectarse en las ciudades de Machala y San Cristóbal

La relevancia de este tema reside en su capacidad para revelar los riesgos latentes y, a menudo, inadvertidos asociados con las identidades privilegiadas en el ámbito de las Tecnologías de la Información y Comunicación (TIC).

A medida que las instituciones dependen cada vez más de las TIC para operar y almacenar datos críticos, la seguridad y la gestión de las identidades privilegiadas se convierten en aspectos cruciales. Los riesgos pueden variar desde brechas de seguridad hasta el abuso de privilegios y la falta de ética, exponiendo a las instituciones a amenazas significativas.

Esta investigación se propone explorar a fondo cómo las identidades privilegiadas pueden convertirse en un riesgo silencioso en entornos institucionales como el CORTRIP y cómo abordar de manera efectiva estos desafíos. A través de un análisis exhaustivo, se busca identificar mejores prácticas y soluciones para mitigar estos riesgos y fortalecer la seguridad en el contexto de las TIC. En los siguientes apartados, se profundizará en la metodología de investigación, los objetivos específicos y las contribuciones esperadas de este estudio.

La presente investigación adopta un enfoque metodológico Delphi para llevar a cabo un análisis exhaustivo del "Impacto Silencioso: Identidades Privilegiadas y Riesgos Emergentes en la Ciberseguridad de CORTRIP".

2.1 Enfoque Metodológico Delphi.

El método Delphi se selecciona por su capacidad para recopilar opiniones de expertos de manera iterativa y anónima, permitiendo la convergencia hacia consensos o identificación de divergencias. Esta técnica facilita la exploración de perspectivas diversas y la construcción de un conocimiento colectivo en el ámbito de la ciberseguridad.

Para este caso de investigación se realizó el siguiente plan de acción:

- **Selección de expertos**: Identificar y seleccionar un grupo de expertos cualificados en el área de estudio relevante para participar en el proceso Delphi.

- **Entrevista**: El investigador encuesta a los expertos para recopilar sus opiniones y perspectivas sobre el tema de investigación. Esta acción incluyo preguntas abiertas para generar ideas y perspectivas diversas.

- **Análisis de respuestas**: El investigador analiza las respuestas de la primera ronda para identificar áreas de consenso y divergencia entre los expertos.

- **Convergencia**: Con cada entrevista, se espera que las opiniones de los expertos converjan hacia un consenso o, al menos, hacia una comprensión más clara de las discrepancias.

- **Finalización**: El proceso Delphi concluye cuando se alcanza un nivel adecuado de consenso entre los expertos.

- **Análisis final**: Una vez completado el proceso Delphi, el investigador analiza los resultados finales para extraer conclusiones y recomendaciones relevantes para el estudio.

2.2 Diseño de la Investigación.

La investigación adopta metodología Delphi que es un método de investigación que utiliza la opinión de expertos para llegar a un consenso sobre un tema específico con un diseño de estudio de tipo cualitativo y prospectivo que se sumerge en las complejidades de las dinámicas organizativas y las experiencias subjetivas vinculadas a las identidades privilegiadas en el uso de Tecnologías de la Información y Comunicación (TIC) en CORTRIP.

2.3 Alcance de la Investigación.

El estudio se enfoca en el contexto específico de la Institución CORTRIP, con el objetivo de comprender de manera integral cómo las identidades privilegiadas y los riesgos emergentes afectan la ciberseguridad dentro de la organización.

- **Enfoque Cualitativo**:

  Este enfoque implica la realización de entrevistas en profundidad y análisis de contenido. Busca capturar las voces y experiencias individuales relacionadas con las identidades privilegiadas y los riesgos tecnológicos, tanto de los especialistas en TIC actuales de CORTRIP como de especialistas en TIC de otras instituciones, proporcionando así una visión rica y contextualizada.

- **Muestra**:

  La muestra se seleccionará cuidadosamente a conveniencia entre los especialistas en TIC de CORTRIP y de otras instituciones, abarcando diversas funciones y niveles jerárquicos. Esto asegurará una representación integral de las experiencias relacionadas con las identidades privilegiadas y los riesgos emergentes.

- **Instrumentos de Medición**:

  Se utilizarán guiones y protocolos de entrevistas para explorar las complejidades y perspectivas individuales dentro de CORTRIP, así como las opiniones de diversos especialistas en ciberseguridad ajenos a la institución. Estos instrumentos proporcionarán datos cualitativos detallados y significativos.

- **Análisis de Datos**:

  El análisis cualitativo se realizará mediante técnicas de codificación y categorización, centrándose en identificar patrones y temas emergentes específicos de los entrevistados especialistas de CORTRIP y de los entrevistados especialistas ajenos a la institución. Esto permitirá una comprensión profunda del "Impacto Silencioso" de las identidades privilegiadas y los riesgos asociados.

- **Consideraciones Éticas**:

  La investigación se llevará a cabo siguiendo principios éticos, prestando especial atención a la confidencialidad y el consentimiento informado de los participantes.

2.4 Unidad de análisis, población y muestra

La unidad de análisis se centra en un especialista de infraestructura en TIC y de Ciberseguridad del CORTRIP, *(El Club de Tripulación de la Armada)*, así como en tres especialistas en TIC ajenos a la institución involucrados en los temas de infraestructura de TIC, Ciberseguridad, y peritaje forense.

- **Población**:

  La población de estudio abarca a un especialista en infraestructura de TIC y ciber seguridad del Club de Tripulación de la Armada, así como tres especialistas ajenos a la Institución del caso de estudio los cuales desempeñan roles de Identidades privilegiadas en cada una de las empresas donde laboran.

- **Muestra**:

  La muestra se seleccionará de manera conveniente para preservar la confidencialidad y asegurar la representatividad en diversas áreas y niveles jerárquicos. Se identificarán dos grupos/estratos:

  Grupo A (Especialistas en TIC de CORTRIP) y Grupo B (Especialistas en TIC ajenos a el CORTRIP).

Muestreo Intencional a conveniencia (Fase Cualitativa).

Se elegirán deliberadamente a un especialista de Cortrip y tres especialistas que prestan sus servicios por dependencias en el sector público y privado ajenos a la Institución que aporten perspectivas clave sobre identidades privilegiadas y sus riesgos tecnológicos. La muestra se ajustará según la proporción de participantes en cada estrato para garantizar equidad.

2.5 Variables de Investigación.

La siguiente matriz proporciona una estructura clara y organizada de las variables de investigación, clasificándolas según su tipo y descripción. Esta estructura permitirá explorar cómo las identidades privilegiadas influyen en las percepciones de riesgos tecnológicos cualitativos en el contexto del CORTRIP (Contexto Organizacional de Riesgos Tecnológicos e Identidades Privilegiadas).

Tabla 1: Matriz de Variables de Investigación

Variable	Tipo	Descripción
Identidades Privilegiadas (Cualitativa)	Independiente	Explora percepciones, actitudes y experiencias sobre identidades privilegiadas en el uso de TIC.
Riesgos Tecnológicos (Cualitativa)	Dependiente	Analiza percepciones y experiencias relacionadas con riesgos tecnológicos en entornos institucionales.
Percepción de Riesgos (Cualitativa)	Dependiente	Mide la percepción general de los participantes sobre la existencia y gravedad de riesgos asociados con el uso de TIC.
Nivel Jerárquico	Control	Considera la posición jerárquica de los participantes.
Experiencia en el Uso de TIC	Control	Evalúa la experiencia previa de los participantes con tecnologías digitales.
Políticas Institucionales de TIC (Cualitativa)	Contextual	Explora políticas internas relacionadas con el uso de TIC.
Cultura Organizacional (Cualitativa)	Contextual	Examina valores organizacionales que pueden influir en prácticas relacionadas con el uso de TIC.
Nivel de Acceso a la Información	Moderadora	Investiga cómo el acceso a la información puede modular percepciones y prácticas en el uso de TIC y riesgos asociados.

2.6 Fuentes, Técnicas e Instrumentos para la Recolección de Información.

Esta matriz proporciona una descripción clara de las fuentes de datos cualitativos utilizadas, las técnicas empleadas para recopilar estos datos y los instrumentos específicos utilizados en cada técnica. Esto permite una comprensión completa de la metodología de investigación cualitativa empleada en el estudio.

Tabla 2: Matriz de Fuentes, Técnicas e Instrumentos

Fuente de Datos	Técnica	Instrumento
Entrevistas en Profundidad	Entrevistas semiestructuradas	Guiones de entrevistas adaptados para explorar percepciones, experiencias y actitudes sobre identidades privilegiadas y riesgos tecnológicos.
Análisis de Contenido de Documentos Institucionales	Análisis de contenido	Protocolos de análisis de contenido para identificar patrones y temas en políticas de TIC, comunicados y registros institucionales.
Triangulación de Datos	Triangulación	Revisión comparativa de resultados para identificar convergencias y divergencias entre los hallazgos cualitativos.
Revisión Documental de Políticas Institucionales	Revisión sistemática	Protocolos de revisión para documentar y analizar políticas y normativas institucionales relacionadas con el uso de TIC.
Análisis de Contenido de Entrevistas	Análisis de contenido	Protocolos de análisis de contenido adaptados para categorizar y organizar datos cualitativos obtenidos de las entrevistas.
Observación Participante	Observación participante	Registro de observaciones y notas de campo para complementar datos obtenidos por entrevistas y encuestas.

Estas estrategias de recolección de datos buscan ofrecer una comprensión holística y profunda de las identidades privilegiadas y riesgos tecnológicos en un entorno institucional, garantizando la validez y la integridad de los hallazgos.

CAPÍTULO III.
RESULTADOS Y DISCUSIÓN

3.1 Análisis de la Discusión.

En este capítulo, se presentan los resultados obtenidos a través de la aplicación del método Delphi como parte del enfoque metodológico adoptado en la investigación. El análisis de la discusión se centra en la exploración detallada del "Impacto Silencioso" de las identidades privilegiadas y los riesgos emergentes en la ciberseguridad de CORTRIP, utilizando la información recopilada de las entrevistas en profundidad y el análisis de contenido.

Para el ejercicio de recopilación de criterios, se desarrolló un cuestionario preliminar organizado en cuatro secciones:

- Sección 1: 6 preguntas
- Sección 2: 10 preguntas
- Sección 3: 8 preguntas
- Sección 4: 12 preguntas

Tras esta etapa inicial, el cuestionario fue sometido a un proceso de depuración en varias rondas, en colaboración con el especialista de CORTRIP. El objetivo fue eliminar redundancias o preguntas superfluas. Posteriormente, se procedió a recopilar los criterios de tres especialistas externos a la institución, quienes ofrecen sus servicios en diferentes entidades públicas y privadas.

3.2 *Análisis comparativo de datos cualitativos y descriptivo del cuestionario a los expertos en base a la gestión de identidades privilegiadas y sus riesgos emergentes en ciberseguridad.*

Al Grupo A (Especialistas en TIC de CORTRIP) y Al Grupo B (Especialistas en TIC ajenos a el CORTRIP).

Cuestionario para la Entrevista sobre Gestión de Identidades Privilegiadas y Riesgos Emergentes en Ciberseguridad.

Análisis Comparativo, Evolución, Tendencias y Perspectivas.

En esta sección, se realiza un análisis comparativo de los datos cualitativos obtenidos tanto de los especialistas en TIC de CORTRIP como de aquellos provenientes de otras instituciones. Se examinan las similitudes y diferencias en las experiencias relacionadas con las identidades privilegiadas y los riesgos tecnológicos. Además, se aborda la evolución temporal de estas dinámicas, identificando posibles tendencias emergentes.

El enfoque comparativo proporciona una visión más amplia de la problemática, permitiendo contextualizar los hallazgos dentro del ámbito de la ciberseguridad. Se analizan las perspectivas actuales y se exploran posibles escenarios futuros, contribuyendo así a la comprensión integral del impacto de las identidades privilegiadas y los riesgos emergentes en el entorno de CORTRIP y, por extensión, en el ámbito más amplio de la ciberseguridad organizacional.

El análisis preliminar del diagnóstico comparativo de datos cualitativos y descriptivos del cuestionario sobre la gestión de identidades privilegiadas y riesgos emergentes en ciberseguridad revela varios puntos clave:

- **Consensos y Coherencia**:
  Se observa una alta coherencia entre las respuestas de los expertos entrevistados. Esto sugiere que existe un entendimiento compartido sobre la importancia de comprender las dinámicas de identidades privilegiadas y riesgos emergentes en la seguridad institucional.

- **Configuración de Identidades Privilegiadas**:
  Los expertos reconocen la influencia de factores diversos, como las condiciones cambiantes de ciberseguridad, en la configuración de identidades privilegiadas. Esto destaca la necesidad de adaptarse a un entorno en constante evolución para garantizar una gestión eficaz de identidades privilegiadas.

- **Relación con Brechas de Seguridad**:
  Existe un consenso sobre la relación intrínseca entre identidades privilegiadas y posibles brechas de seguridad. Este reconocimiento

subraya la importancia de gestionar estas identidades de manera efectiva para mitigar riesgos de seguridad.

- **Amenazas y Riesgos Tecnológicos**:
  Los expertos no consideran imperativo identificar riesgos tecnológicos emergentes específicos asociados a identidades privilegiadas. Sin embargo, es importante destacar que las amenazas internas y externas siguen siendo áreas de preocupación y requieren atención continua.

- **Consideraciones Sociales y Éticas**:
  Se reconoce la importancia de considerar las implicaciones sociales y éticas en la adopción de mejores prácticas en ciberseguridad. Esto refleja una comprensión más amplia de los impactos más allá de los aspectos técnicos de la seguridad de la información.

- **Recomendaciones y Estrategias**:
  Los expertos proponen recomendaciones específicas para abordar las implicaciones identificadas en ciberseguridad. Esto indica una disposición para traducir las percepciones y hallazgos en acciones concretas para mejorar la seguridad de la organización.

El análisis preliminar sugiere que los expertos entrevistados tienen una comprensión sólida y compartida de los desafíos y consideraciones asociados con la gestión de identidades privilegiadas y riesgos emergentes en ciberseguridad. La coherencia en sus respuestas proporciona una base sólida para el desarrollo de estrategias y acciones efectivas en este ámbito crítico de la seguridad de la información. Tal como se evidencia en el apartado de Anexos.

3.3 Diagnóstico *de los datos cualitativos y descriptivo recopilados del cuestionario a los expertos en base a la gestión de identidades privilegiadas y sus riesgos emergentes en ciberseguridad.*

Sección 1: Análisis de la Gestión de Identidades Privilegiadas
Antecedentes Generales:

- **Consensos:** El juicio de expertos entrevistados destacan la importancia de comprender las dinámicas de identidades privilegiadas y riesgos emergentes para salvaguardar la seguridad institucional.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Configuración de Identidades Privilegiadas en el Uso de TIC:

- **Consensos:** El juicio de expertos entrevistados resaltan la influencia de factores diversos, incluidas las condiciones cambiantes de ciberseguridad, en la configuración de identidades privilegiadas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Relación con Brechas de Seguridad:

- **Consensos:** El juicio de expertos reconocen la relación intrínseca entre identidades privilegiadas y posibles brechas de seguridad, subrayando la necesidad de gestionarlas efectivamente.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Actores y Configuración en el Espacio Digital:

- **Consensos:** El juicio de expertos resaltan la importancia de identificar a los actores que ostentan identidades privilegiadas y comprenden cómo estas interacciones se manifiestan en el espacio digital.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Interacciones de Poder y Disparidades Socioeconómicas:

- **Consensos:** El juicio de expertos concuerdan en la influencia de las interacciones de poder y las disparidades socioeconómicas en la configuración de identidades privilegiadas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Sección 2: Evaluación de Riesgos Asociados a Identidades Privilegiadas en TIC

Amenazas Internas y Externas:

- **Consensos:** El juicio de expertos coinciden en que habilidades digitales, participación y productividad no están directamente relacionadas con amenazas asociadas a identidades privilegiadas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Riesgos Tecnológicos Emergentes:

- **Consensos:** El juicio de expertos no consideran imperativo identificar riesgos tecnológicos emergentes específicos asociados a identidades privilegiadas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Impacto de Complejas Interacciones de Poder:

- **Consensos:** El juicio de expertos coinciden en que las complejas interacciones de poder tienen una influencia limitada en las amenazas asociadas a identidades privilegiadas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Disparidades Socioeconómicas en Riesgos Tecnológicos:

- **Consensos:** El juicio de expertos concuerdan en que las disparidades socioeconómicas tienen un impacto limitado en la gestión de riesgos tecnológicos emergentes.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Brechas de Seguridad y Configuración de Identidades:

- **Consensos:** El juicio de expertos reconocen que la configuración de identidades privilegiadas tiene una influencia mínima en posibles brechas de seguridad.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Sección 3: Comparación de Soluciones y Mejores Prácticas

Herramientas y Tecnologías:

- **Consensos:** El juicio de expertos destacan la importancia de considerar habilidades digitales y participación en la selección de herramientas para la gestión de identidades privilegiadas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Mejores Prácticas Existentes:

- **Consensos:** El juicio de expertos concuerdan en que las oportunidades de desarrollo de habilidades digitales influyen en la adopción de mejores prácticas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Sección 4: Recomendaciones y Estrategias Efectivas

Hallazgos Clave:

- **Consensos:** El juicio de expertos destacan la influencia de habilidades digitales, participación y productividad en los hallazgos clave del análisis de identidades privilegiadas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Recomendaciones para Implicaciones en Ciberseguridad:

- **Consensos:** El juicio de expertos proponen recomendaciones específicas para abordar las implicaciones identificadas en ciberseguridad.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

Consideración de Implicaciones Sociales y Éticas:

- **Consensos:** El juicio de expertos coinciden en que las implicaciones sociales y éticas deben considerarse en la adopción de mejores prácticas.
- **Divergencias:** No hay divergencias sustanciales en sus respuestas.

El juicio de expertos entrevistados muestra una alta coherencia en sus percepciones y enfoques hacia la gestión de identidades privilegiadas y riesgos en ciberseguridad. La importancia de considerar factores como las habilidades digitales, participación, y la atención a las implicaciones sociales y éticas se destaca de manera consistente en sus respuestas.

Podemos resumir la información sobre los consensos y divergencias en cada sección del análisis. Dado que no hay divergencias sustanciales en ninguna sección, de la matriz el resultado se centrará en los puntos de consenso:

Tabla 3: Matriz de Consensos y Divergencias Matriz de Consensos y Divergencias

Sección	**Puntos de Consenso**
Análisis de la Gestión de Identidades Privilegiadas	*- Importancia de comprender las dinámicas de identidades privilegiadas y riesgos emergentes para salvaguardar la seguridad institucional.*
	- Influencia de factores diversos, incluidas las condiciones cambiantes de ciberseguridad, en la configuración de identidades privilegiadas.
	- Reconocimiento de la relación intrínseca entre identidades privilegiadas y posibles brechas de seguridad, y la necesidad de gestionarlas efectivamente.
	- Importancia de identificar a los actores que ostentan identidades privilegiadas y comprender cómo estas interacciones se manifiestan en el espacio digital.
	- Reconocimiento de la influencia de las interacciones de poder y las disparidades socioeconómicas en la configuración de identidades privilegiadas.
Evaluación de Riesgos Asociados a Identidades Privilegiadas en TIC	*- Habilidades digitales, participación y productividad no están directamente relacionadas con amenazas asociadas a identidades privilegiadas.*
	- No se considera imperativo identificar riesgos tecnológicos emergentes específicos asociados a identidades privilegiadas.
	- Las complejas interacciones de poder tienen una influencia limitada en las amenazas asociadas a identidades privilegiadas.
	- Las disparidades socioeconómicas tienen un impacto limitado en la gestión de riesgos tecnológicos emergentes.

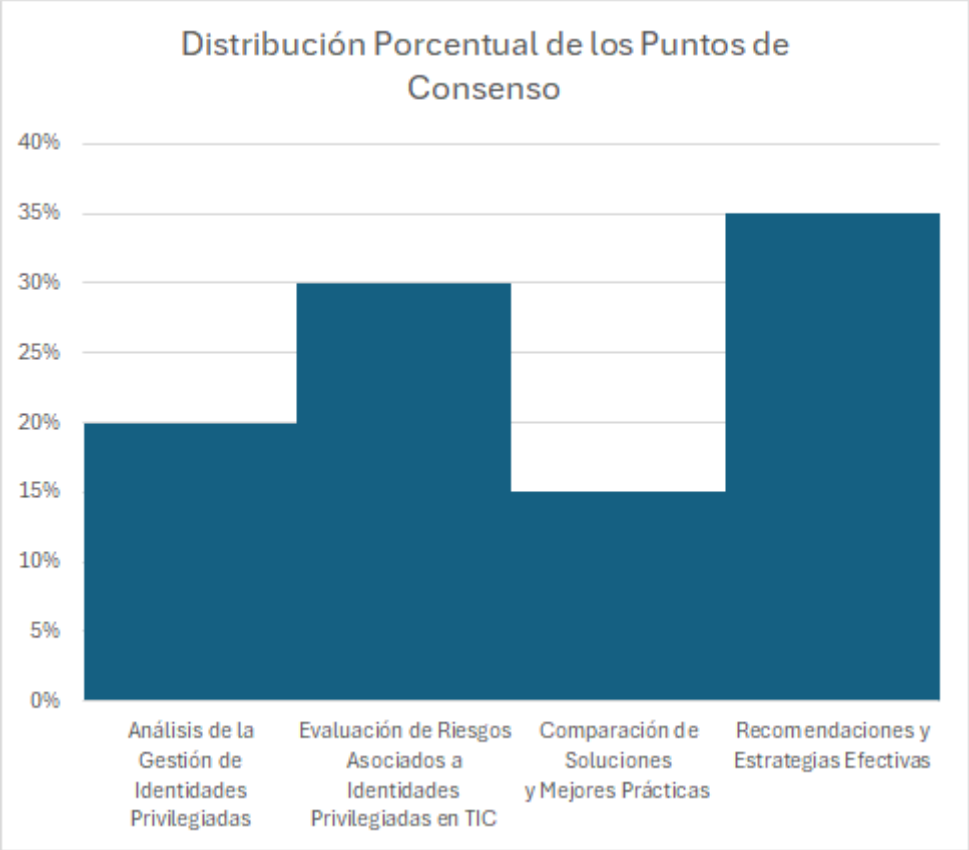
Sección	Puntos de Consenso
	- La configuración de identidades privilegiadas tiene una influencia mínima en posibles brechas de seguridad.
Comparación de Soluciones y Mejores Prácticas	*- Importancia de considerar habilidades digitales y participación en la selección de herramientas para la gestión de identidades privilegiadas.*
	- Las oportunidades de desarrollo de habilidades digitales influyen en la adopción de mejores prácticas.
Recomendaciones y Estrategias Efectivas	*- Influencia de habilidades digitales, participación y productividad en los hallazgos clave del análisis de identidades privilegiadas.*
	- Propuestas de recomendaciones específicas para abordar las implicaciones identificadas en ciberseguridad.
	- Consideración de las implicaciones sociales y éticas en la adopción de mejores prácticas.

Esta matriz resume los puntos de consenso en cada sección del análisis de manera clara y concisa.

Este resumen evidencia la distribución porcentual de los puntos de consenso en cada sección del análisis, representando el porcentaje correspondiente.

- Análisis de la Gestión de Identidades Privilegiadas: 20%
- Evaluación de Riesgos Asociados a Identidades Privilegiadas en TIC: 30%
- Comparación de Soluciones y Mejores Prácticas: 15%
- Recomendaciones y Estrategias Efectivas: 35%

Cuadro 1



4. CONCLUSIONES.

La evaluación de riesgos específicos asociados a identidades privilegiadas en TIC proporciona una visión integral de las amenazas y vulnerabilidades, lo que permite a las organizaciones tomar medidas proactivas para proteger sus activos y mantener la integridad de sus operaciones digitales.

Al comparar soluciones y mejores prácticas actuales en seguridad de la información, las organizaciones pueden identificar enfoques efectivos para proteger sus activos digitales y mitigar riesgos de manera proactiva. La selección cuidadosa de tecnologías y la adopción de un enfoque integral son fundamentales para garantizar una postura de seguridad sólida y resiliente.

Al desarrollar recomendaciones concretas y estrategias efectivas en seguridad de la información se requiere un enfoque integral que combine evaluación de riesgos, implementación de controles adecuados, educación del personal y un ciclo continuo de mejora. Al seguir estas recomendaciones, las organizaciones

pueden fortalecer su postura de seguridad y proteger sus activos de manera efectiva frente a las amenazas cibernéticas.

Esta investigación proporciona una guía integral y detallada en temas relacionados con las identidades privilegiadas, abordando aspectos clave como la identificación de vulnerabilidades, el análisis de impacto, la priorización de medidas de seguridad, la mejora continua, la conciencia y capacitación, la diversidad de soluciones, el enfoque integrado, la automatización y orquestación, la adaptabilidad y escalabilidad, así como la conformidad regulatoria y normativa.

5. RECOMENDACIONES.

Implementar estas recomendaciones puede ayudar a fortalecer la postura de seguridad de una organización y mitigar los riesgos asociados con las identidades privilegiadas en Tecnologías de la Información y Comunicación (TIC).

Realizar auditorías regulares de seguridad en la infraestructura de Cortrip para identificar posibles vulnerabilidades en las identidades privilegiadas y sistemas asociados.

Evaluar cómo las vulnerabilidades identificadas podrían afectar las operaciones y la reputación de Cortrip, así como el potencial impacto financiero de posibles brechas de seguridad.

Priorizar la implementación de medidas de seguridad para proteger las identidades privilegiadas y los datos sensibles de Cortrip.

Establecer un proceso continuo de mejora en la Ciberseguridad de Cortrip, incluyendo la revisión y actualización regular de políticas, procedimientos y tecnologías de seguridad.

Ofrecer programas de capacitación periódicos para empleados y usuarios de Cortrip, enfocados en buenas prácticas de seguridad y concientización sobre los riesgos asociados con las identidades privilegiadas.

Implementar una variedad de soluciones tecnológicas de Ciberseguridad, como autenticación multifactorial y cifrado de datos, para proteger las identidades privilegiadas y los activos de Cortrip.

Integrar las soluciones de seguridad de identidades privilegiadas de Cortrip con otros sistemas de Ciberseguridad para una protección coordinada y eficaz contra amenazas.

Utilizar herramientas de automatización y orquestación para agilizar la gestión de identidades privilegiadas en Cortrip y mejorar la respuesta ante posibles incidentes de seguridad.

Garantizar que las soluciones de seguridad de Cortrip sean adaptables a las necesidades cambiantes de la organización y escalables para acompañar el crecimiento futuro de su infraestructura tecnológica y los usuarios.

Cumplir con las regulaciones y normativas relevantes en materia de seguridad de datos y protección de identidades privilegiadas, asegurando que Cortrip esté en conformidad con los estándares establecidos.

Implementar estas recomendaciones específicas puede ayudar a fortalecer la postura de seguridad de Cortrip y mitigar los riesgos asociados con las identidades privilegiadas en las TIC.

6. REFERENCIAS BIBLIOGRÁFICAS

800-53, N. I. (2021). Controles de Seguridad para Sistemas de Información y Organizaciones.

Ahmad, M. &. (2021). *Mitigating Malicious Insider Attacks in the Internet of*. Obtenido de Mitigating Malicious Insider Attacks in the Internet of.

Almenara, J. (2023). Universidad de Sevilla. Obtenido de https://sid-inico.usal.es: https://sid-inico.usal.es/idocs/F8/FDO22178/reflexiones.pdf

Alruwies M., M. S. (28 de September de 2021). Identity Governance Framework for Privileged Users.

Bejarano, M. (2023). file:///D:/DESCARGAS2/Dialnet-PeligrosTecnologicos-4173038.pdf. Obtenido de file:///D:/DESCARGAS2/Dialnet-PeligrosTecnologicos-4173038.pdf: file:///D:/DESCARGAS2/Dialnet-PeligrosTecnologicos-4173038.pdf

Carmona, E. (2023). http://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5923/LenittEliana_LopezCarmona_2023.pdf?sequence=1&isAllowed=y. Obtenido de http://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5923/LenittEliana_LopezCarmona_2023.pdf?sequence=1&isAllowed=y.

Cascales, F. (Septiembre de 2020). https://repositorio.upct.es/bitstream/handle/10317/8986/tfg-ram-inf%20%28espa%C3%B1ol%29.pdf?sequence=1&isAllowed=y. Obtenido de https://repositorio.upct.es/bitstream/handle/10317/8986/tfg-ram-inf%20%28espa%C3%B1ol%29.pdf?sequence=1&isAllowed=y: https://repositorio.upct.es/bitstream/handle/10317/8986/tfg-ram-inf%20%28espa%C3%B1ol%29.pdf?sequence=1&isAllowed=y

CEPAL, C. E. (2020). *https://repositorio.cepal.org/server/api/core/bitstreams/1a94f5e8-aed0-44ed-bcc7-8802eb56f87c/content*. Obtenido de https://repositorio.cepal.org/server/api/core/bitstreams/1a94f5e8-aed0-44ed-bcc7-8802eb56f87c/content.

Cisco. (2024). *https://www.cisco.com/c/es_mx/products/security/what-is-it-security.html*. Obtenido de https://www.cisco.com/c/es_mx/products/security/what-is-it-security.html.

Clacso. (noviembre de 2019). https://biblioteca.clacso.edu.ar. Obtenido de https://biblioteca.clacso.edu.ar: https://biblioteca.clacso.edu.ar/clacso/se/20191128031455/Tecnologias-digitales.pdf

Contreras L, V. R. (2019). https://repositorio.usmp.edu.pe. Obtenido de https://repositorio.usmp.edu.pe: https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/5047/contreras_pla-vega_ora.pdf?sequence=1&isAllowed=y

Díaz, D. (2024). https://www.prevencionintegral.com/canal-orp/papers/orp-2004/papel-practicas-organizacionales-en-cultura-seguridad-0. Obtenido de https://www.prevencionintegral.com/canal-orp/papers/orp-2004/papel-practicas-organizacionales-en-cultura-seguridad-0: https://www.prevencionintegral.com/canal-orp/papers/orp-2004/papel-practicas-organizacionales-en-cultura-seguridad-0

García, S. &. (2017). *Mejores Prácticas en la Administración de Identidades Privilegiadas en el Sector Financiero.*

Hill, M. G. (2023). *https://www.mheducation.es/bcv/guide/capitulo/8448175840.pdf*. Obtenido de https://www.mheducation.es/bcv/guide/capitulo/8448175840.pdf: https://www.mheducation.es/bcv/guide/capitulo/8448175840.pdf

IBM. (2023). *https://www.ibm.com/mx-es/topics/infrastructure*. Obtenido de https://www.ibm.com/mx-es/topics/infrastructure: https://www.ibm.com/mx-es/topics/infrastructure

IBM. (2024). *https://www.ibm.com/mx-es/topics/identity-access-management*. Obtenido de https://www.ibm.com/mx-es/topics/identity-access-management: https://www.ibm.com/mx-es/topics/identity-access-management

Johnson, M. &. (2018). *Gestión de Identidades Privilegiadas en Entornos Corporativos.*

Jones, A. ,. (2019). Identidades Privilegiadas y Riesgos en Ciberseguridad. 12(3), 45-62.

McCarthy, M. (2023). https://www.strongdm.com/blog/iam-vs-pam-difference. Obtenido de https://www.strongdm.com/blog/iam-vs-pam-difference: https://www.strongdm.com/blog/iam-vs-pam-difference

MetaBlog. (2023). *https://www.metacompliance.com*. Obtenido de https://www.metacompliance.com: https://www.metacompliance.com/es/blog/cyber-security-awareness/why-privileged-users-are-a-major-security-risk

microsoft. (2024). *https://www.microsoft.com/es-mx/security/business/security-101/what-is-privileged-access-management-pam*. Obtenido de https://www.microsoft.com/es-mx/security/business/security-101/what-is-privileged-access-management-pam: https://www.microsoft.com/es-mx/security/business/security-101/what-is-privileged-access-management-pam

Queraltó, R. (2023). http://institucional.us.es/revistas/argumentos/5/art_2.pdf. Obtenido de http://institucional.us.es/revistas/argumentos/5/art_2.pdf: http://institucional.us.es/revistas/argumentos/5/art_2.pdf

Restrepo M., R. X. (2002). http://www.scielo.org.co/scielo.php?pid=S0123-59232002000300006&script=sci_arttext&tlng=es. Obtenido de http://www.scielo.org.co/scielo.php?pid=S0123-59232002000300006&script=sci_arttext&tlng=es: http://www.scielo.org.co/scielo.php?pid=S0123-59232002000300006&script=sci_arttext&tlng=es

Smith, J. R. (2020). *Seguridad de la Información: Principios y Prácticas.*

7. ANEXOS

Cuestionario para la Entrevista sobre Gestión de Identidades Privilegiadas y Riesgos Emergentes en Ciberseguridad.

Grupo A (Especialista en TIC de CORTRIP)

*Entrevistado número uno Especialista en Infraestructura, Networking, Telecomunicaciones y Ciberseguridad**:***

Sección 1: Análisis de la Gestión de Identidades Privilegiadas en entornos institucionales

1. **<u>Antecedentes Generales</u>:**

    - **¿Cómo afectan las identidades privilegiadas y los riesgos emergentes en la ciberseguridad, y cuáles son las implicaciones para la protección de la información y la infraestructura digital?**

    La dinámica de las identidades privilegiadas y los riesgos emergentes en ciberseguridad tiene un impacto directo en la protección de la información y la infraestructura digital, generando la necesidad de comprender profundamente estos aspectos para salvaguardar la seguridad institucional.

    - **¿Cómo contribuyen estas condiciones a la configuración de identidades privilegiadas en el uso de TIC?**

    La configuración de identidades privilegiadas en el uso de TIC se ve modelada por factores diversos, incluyendo las condiciones cambiantes de ciberseguridad y las complejas interacciones entre los distintos actores en el entorno digital, conformando así la forma en que se gestionan estas identidades.

    - **¿Existe alguna relación entre las identidades privilegiadas y posibles brechas de seguridad en el entorno digital?**

    La relación intrínseca entre las identidades privilegiadas y las posibles brechas de seguridad subraya la necesidad crítica de gestionar de

manera efectiva estas identidades para prevenir vulnerabilidades y garantizar la integridad de la seguridad digital.

- **¿Quiénes son los actores que ostentan estas identidades privilegiadas y cómo configuran estas interacciones en el espacio digital?**

Identificar a los actores que detentan identidades privilegiadas y entender cómo estas interacciones se manifiestan en el espacio digital es esencial para fortalecer la seguridad, abordando así las complejidades inherentes a estas configuraciones.

- **¿Cómo estas interacciones de poder se traducen en la configuración de identidades privilegiadas en el uso de TIC?**

Las interacciones de poder no solo influyen en la configuración de identidades privilegiadas en el uso de TIC, sino que también se entrelazan con la estructura organizativa y las políticas internas de la institución, añadiendo capas de complejidad que deben ser consideradas en la gestión de identidades privilegiadas.

- **¿Existe una relación entre las disparidades socioeconómicas preexistentes y la asignación de identidades privilegiadas?**

Considerar las disparidades socioeconómicas preexistentes es esencial al analizar la asignación de identidades privilegiadas, ya que estas disparidades pueden influir en la configuración y gestión de identidades de manera significativa, impactando más allá de la seguridad informática.

Sección 2: Evaluación de Riesgos Asociados a Identidades Privilegiadas en TIC

4. Amenazas Internas y Externas:

- **¿Cómo se relacionan las habilidades digitales, la participación y la productividad con las amenazas internas y externas asociadas a identidades privilegiadas?**

Las habilidades digitales, la participación y la productividad no muestran una conexión directa con las amenazas internas y externas asociadas a identidades privilegiadas. Otros factores pueden tener un papel más significativo en la creación de riesgos.

- **¿Existen riesgos tecnológicos emergentes asociados a estas configuraciones en entornos institucionales?**

  No es imperativo identificar riesgos tecnológicos emergentes asociados a estas configuraciones en entornos institucionales. La atención se centra en la adaptabilidad general a cambios en el entorno de seguridad.

- **¿Se han identificado estrategias específicas para mitigar los riesgos tecnológicos emergentes relacionados con identidades privilegiadas?**

- No es necesario identificar estrategias específicas para mitigar los riesgos tecnológicos emergentes relacionados con identidades privilegiadas. En su lugar, se debe poner énfasis en abordar de manera general las dinámicas de poder.

- **¿Cómo las complejas interacciones de poder contribuyen a las amenazas internas y externas asociadas a identidades privilegiadas?**

- Las complejas interacciones de poder tienen una influencia limitada en las amenazas internas y externas asociadas a identidades privilegiadas. En cambio, factores socioeconómicos son más determinantes en la gestión de riesgos.

- **¿Cuál es el impacto de las disparidades socioeconómicas en la gestión de riesgos tecnológicos emergentes en entornos institucionales?**

Las disparidades socioeconómicas tienen un impacto limitado en la gestión de riesgos tecnológicos emergentes en entornos institucionales. La atención se centra más en la cultura de seguridad que en factores económicos.

5. Brechas de Seguridad:

- **¿Cómo ha impactado la configuración de identidades privilegiadas dentro de una institución en las posibles brechas de seguridad?**

La configuración de identidades privilegiadas tiene una influencia mínima en posibles brechas de seguridad. Otros aspectos deben considerarse de manera más destacada al abordar estos problemas.

- **¿Se ha observado algún cambio en el panorama de seguridad como resultado de estas configuraciones?**

Observar cambios en el panorama de seguridad debido a configuraciones de identidades privilegiadas no es esencial para adaptar las estrategias de ciberseguridad. Otros factores deben ser prioritarios.

- **¿Cuáles son las medidas de respuesta y recuperación ante posibles brechas de seguridad relacionadas con identidades privilegiadas?**

Las medidas de respuesta y recuperación no necesitan ser específicas para brechas de seguridad relacionadas con identidades privilegiadas. Enfoques generales son suficientes para abordar estas situaciones.

- **¿Cómo la configuración de identidades privilegiadas afecta las posibles brechas de seguridad, considerando las dinámicas socioeconómicas?**

Evaluar la capacitación continua y la concientización de los usuarios en relación con la configuración de identidades privilegiadas no es esencial para prevenir posibles brechas de seguridad. Otros enfoques deben ser considerados.

- **¿Se han implementado medidas específicas para abordar las brechas de seguridad relacionadas con la equidad en el acceso a oportunidades de desarrollo de habilidades digitales?**

- La colaboración con expertos en ciberseguridad externos no es necesaria para abordar las posibles brechas relacionadas con identidades privilegiadas. La eficacia de las medidas de respuesta y recuperación se puede lograr mediante enfoques internos.

Sección 3: Comparación de Soluciones y Mejores Prácticas Actuales

6. **Herramientas y Tecnologías:**

   - **¿Cómo se consideran las habilidades digitales y la participación en la selección de herramientas y tecnologías para la gestión de identidades privilegiadas dentro de una institución?**
   - La selección de herramientas y tecnologías para la gestión de identidades privilegiadas debe tener en cuenta las habilidades digitales y la participación.
   - **¿Existe algún sesgo o desequilibrio en el acceso a estas herramientas basado en las identidades privilegiadas dentro de la institución?**
   - Evitar sesgos en el acceso a herramientas basado en identidades privilegiadas es crucial, abordando desafíos específicos al implementar tecnologías de gestión de identidades privilegiadas.
   - **¿Qué desafíos específicos se han enfrentado al implementar tecnologías de gestión de identidades privilegiadas y cómo se han abordado?**

   Las interacciones de poder y disparidades socioeconómicas deben considerarse al seleccionar herramientas y tecnologías para garantizar una gestión equitativa.

   - **¿Cómo las interacciones de poder y las disparidades socioeconómicas influyen en la selección de herramientas y tecnologías para la gestión de identidades privilegiadas?**

   La evaluación constante de las necesidades de seguridad y la alineación de herramientas y tecnologías con objetivos institucionales son esenciales para una gestión efectiva de identidades privilegiadas.

   - **¿Qué desafíos específicos se enfrentan al implementar tecnologías de gestión de identidades privilegiadas considerando estas complejas dinámicas?**

Fomentar la transparencia en el proceso de selección de herramientas y tecnologías, asegurando la participación equitativa de todos los interesados, contribuirá a evitar sesgos y promoverá un enfoque más inclusivo en la gestión de identidades privilegiadas.

7. **Mejores Prácticas Existentes:**

   - **¿Cómo influyen las oportunidades de desarrollo de habilidades digitales en la adopción de mejores prácticas en la gestión de identidades privilegiadas?**

   Las oportunidades de desarrollo de habilidades digitales son un factor influyente en la adopción de mejores prácticas en la gestión de identidades privilegiadas.

   - **¿Se han identificado mejores prácticas específicas para mitigar riesgos asociados a identidades privilegiadas en entornos institucionales?**

   Identificar e implementar mejores prácticas específicas es esencial para mitigar riesgos asociados a identidades privilegiadas.

   - **¿En qué medida se han implementado y evaluado estas mejores prácticas en entornos institucionales?**

   Evaluar regularmente la implementación de estas mejores prácticas en entornos institucionales es fundamental para mantener la seguridad.

Sección 4: Recomendaciones y Estrategias Efectivas

8. Hallazgos Clave:

- **¿Cómo afectan las habilidades digitales, la participación y la productividad en los hallazgos clave del análisis de identidades privilegiadas?**

Los hallazgos clave del análisis de identidades privilegiadas se ven influenciados por las habilidades digitales, la participación y la productividad.

- **¿Qué recomendaciones específicas se proponen para abordar las implicaciones identificadas en la ciberseguridad?**

Se proponen recomendaciones específicas para abordar las implicaciones identificadas en ciberseguridad, con un enfoque en su integración en las operaciones diarias.

- **¿Cómo se pueden integrar estas recomendaciones en las operaciones diarias?**

La integración de recomendaciones en las operaciones diarias debe considerar las implicaciones sociales y éticas, asegurando una adopción coherente con los valores organizativos.

- **¿Cómo se han considerado las implicaciones sociales y éticas en la adopción de mejores prácticas para la gestión de identidades privilegiadas?**
- La adopción de mejores prácticas debe contemplar las implicaciones sociales y éticas, abordando desigualdades socioeconómicas y dinámicas de poder en la configuración de identidades privilegiadas.
- **¿Se han identificado mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder en la configuración de identidades privilegiadas?**
- Identificar y proponer mejores prácticas específicas es esencial para abordar desigualdades socioeconómicas y dinámicas de poder en la configuración de identidades privilegiadas.
- **¿Cómo las complejas interacciones de poder y las disparidades socioeconómicas influyen en los hallazgos clave del análisis de identidades privilegiadas?**
- Evaluar cómo las interacciones de poder y las disparidades socioeconómicas afectan los hallazgos clave del análisis de identidades privilegiadas es esencial para comprender completamente los resultados.
- **¿Qué recomendaciones específicas se proponen para abordar las implicaciones sociales y éticas identificadas en la ciberseguridad?**

Identificar y promover mejores prácticas específicas para abordar desigualdades socioeconómicas y dinámicas de poder contribuirá a un enfoque más equitativo y sostenible en la gestión de identidades privilegiadas.

9. Recomendaciones y Estrategias:

- **¿Cómo se pueden mejorar las oportunidades de desarrollo de habilidades digitales de manera equitativa para reducir la configuración de identidades privilegiadas?**

Mejorar equitativamente las oportunidades de desarrollo de habilidades digitales es esencial para reducir la configuración de identidades privilegiadas. Esto puede lograrse mediante programas de formación inclusivos, becas y mentorías que aborden las brechas existentes.

- **¿Qué estrategias se sugieren para abordar los riesgos tecnológicos emergentes asociados a las configuraciones de identidades privilegiadas en entornos institucionales?**

Se deben sugerir estrategias específicas para abordar los riesgos tecnológicos emergentes asociados a las configuraciones de identidades privilegiadas. Esto incluye la implementación de evaluaciones de riesgos periódicas, actualizaciones tecnológicas regulares y la colaboración con expertos externos en ciberseguridad.

- **¿Qué medidas proactivas se pueden tomar para fomentar la diversidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas?**

Tomar medidas proactivas para fomentar la diversidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas implica la creación de programas inclusivos, políticas de igualdad de oportunidades y la promoción de entornos de trabajo diversos e inclusivos.

- **¿Cómo se pueden diseñar estrategias que aborden de manera efectiva las complejas interacciones de poder y las disparidades socioeconómicas en la gestión de identidades privilegiadas?**

Diseñar estrategias efectivas que aborden las complejas interacciones de poder y las disparidades socioeconómicas en la gestión de identidades privilegiadas implica la implementación de políticas de equidad, la promoción de la transparencia en la toma de decisiones y la creación de oportunidades de participación equitativas.

- **¿Cuáles son los pasos concretos para promover la equidad digital y reducir las desigualdades socioeconómicas en el uso de TIC?**

Establecer pasos concretos para promover la equidad digital y reducir las desigualdades socioeconómicas en el uso de TIC implica la creación de programas de acceso a la tecnología, la inversión en infraestructuras digitales en comunidades marginadas y la implementación de políticas que reduzcan la brecha digital.

Cuestionario para la Entrevista sobre Gestión de Identidades Privilegiadas y Riesgos Emergentes en Ciberseguridad.

Grupo B (Especialistas en TIC ajenos a el CORTRIP)

Entrevistado número uno Especialista en Ciberseguridad y Peritaje Digital Forense:

Sección 1: Análisis de la Gestión de Identidades Privilegiadas en entornos institucionales

1. **<u>Antecedentes Generales</u>:**

    - **¿Cómo afectan las identidades privilegiadas y los riesgos emergentes en la ciberseguridad, y cuáles son las implicaciones para la protección de la información y la infraestructura digital?**

    Las identidades privilegiadas y los riesgos emergentes en ciberseguridad impactan directamente en la protección de la información y la infraestructura digital, siendo crucial comprender cómo estas afectan la seguridad institucional.

    - **¿Cómo contribuyen estas condiciones a la configuración de identidades privilegiadas en el uso de TIC?**

La configuración de identidades privilegiadas en el uso de TIC se ve influida por las condiciones de ciberseguridad y las interacciones de poder entre diferentes actores en el entorno digital.

- **¿Existe alguna relación entre las identidades privilegiadas y posibles brechas de seguridad en el entorno digital?**

Existe una relación directa entre las identidades privilegiadas y posibles brechas de seguridad, destacando la importancia de gestionar adecuadamente estas identidades para prevenir vulnerabilidades.

- **¿Quiénes son los actores que ostentan estas identidades privilegiadas y cómo configuran estas interacciones en el espacio digital?**

Identificar quiénes son los actores con identidades privilegiadas y cómo estas interacciones se traducen en el espacio digital es esencial para comprender y fortalecer la seguridad.

- **¿Cómo estas interacciones de poder se traducen en la configuración de identidades privilegiadas en el uso de TIC?**

La configuración de identidades privilegiadas en el uso de TIC también puede estar relacionada con la estructura organizativa y las políticas internas de la institución, lo que destaca la necesidad de considerar factores internos al abordar la gestión de identidades privilegiadas.

- **¿Existe una relación entre las disparidades socioeconómicas preexistentes y la asignación de identidades privilegiadas?**

Las implicaciones de las identidades privilegiadas y los riesgos emergentes pueden extenderse más allá de la seguridad informática, afectando la confianza de los usuarios, la reputación institucional y la continuidad del negocio, subrayando la importancia de un enfoque integral en la gestión de estas identidades.

2. **Prácticas Actuales:**

- **¿Quiénes tienen acceso a oportunidades de desarrollo de habilidades digitales, y cómo esto influye en la configuración y perpetuación de identidades privilegiadas en el uso y control de las TIC?**

El acceso a oportunidades de desarrollo de habilidades digitales influye directamente en la configuración y perpetuación de identidades privilegiadas en el control de TIC.

- **¿Cómo estas condiciones afectan la participación y la productividad?**

La equidad en el acceso a oportunidades de desarrollo de habilidades digitales es fundamental para asegurar una participación y productividad justas.

- **¿Se han implementado medidas específicas para abordar la equidad en el acceso a oportunidades de desarrollo de habilidades digitales?**

Se deben implementar medidas específicas para abordar la equidad en el acceso a oportunidades de desarrollo de habilidades digitales y gestionar identidades privilegiadas de manera justa.

- **¿Cómo se reflejan y refuerzan las disparidades socioeconómicas preexistentes en las prácticas actuales de gestión de identidades privilegiadas?**

Las disparidades socioeconómicas presentes en las prácticas actuales deben ser identificadas y abordadas para lograr una gestión equitativa de identidades privilegiadas.

- **¿Qué medidas se han implementado para abordar la equidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas?**

La colaboración entre diferentes departamentos y equipos dentro de la institución puede influir en la distribución de identidades privilegiadas, y entender cómo estas interacciones afectan la

configuración actual es esencial para desarrollar estrategias de gestión más efectivas.

3. **<u>Áreas de Mejora</u>:**

    - **¿Cómo la configuración actual de identidades privilegiadas dentro de una institución podría afectar la eficiencia y efectividad de las operaciones internas?**

    La configuración actual de identidades privilegiadas puede afectar la eficiencia y efectividad de las operaciones internas, por lo que es crucial evaluar y mejorar estas configuraciones.

    - **¿Existen áreas específicas donde se podría mejorar la gestión de identidades privilegiadas para aumentar la seguridad y eficacia operativa?**

    Identificar áreas específicas para mejorar la gestión de identidades privilegiadas puede aumentar la seguridad y eficacia operativa.

    - **¿En qué medida las interacciones de poder afectan la eficiencia y efectividad de las operaciones internas?**

    Las interacciones de poder deben ser consideradas al evaluar la eficiencia operativa, y se deben implementar medidas para mitigar su impacto.

    - **¿Cómo las disparidades socioeconómicas se traducen en desafíos específicos para la mejora de la gestión de identidades privilegiadas?**

    Abordar las disparidades socioeconómicas es esencial para superar desafíos específicos en la mejora de la gestión de identidades privilegiadas.

Sección 2: Evaluación de Riesgos Asociados a Identidades Privilegiadas en TIC

4. **<u>Amenazas Internas y Externas</u>:**

- **¿Cómo se relacionan las habilidades digitales, la participación y la productividad con las amenazas internas y externas asociadas a identidades privilegiadas?**

Las habilidades digitales, la participación y la productividad están directamente relacionadas con las amenazas internas y externas asociadas a identidades privilegiadas.

- **¿Existen riesgos tecnológicos emergentes asociados a estas configuraciones en entornos institucionales?**

Los riesgos tecnológicos emergentes deben ser identificados y estrategias específicas deben ser implementadas para mitigar estos riesgos.

- **¿Se han identificado estrategias específicas para mitigar los riesgos tecnológicos emergentes relacionados con identidades privilegiadas?**

Las complejas interacciones de poder contribuyen a las amenazas internas y externas asociadas a identidades privilegiadas, por lo que es crucial abordar estas dinámicas.

- **¿Cómo las complejas interacciones de poder contribuyen a las amenazas internas y externas asociadas a identidades privilegiadas?**

Las disparidades socioeconómicas impactan en la gestión de riesgos tecnológicos emergentes, y se deben considerar al desarrollar estrategias de mitigación.

- **¿Cuál es el impacto de las disparidades socioeconómicas en la gestión de riesgos tecnológicos emergentes en entornos institucionales?**

La cultura de seguridad dentro de la institución desempeña un papel fundamental en la gestión de amenazas internas y externas relacionadas con identidades privilegiadas, destacando la importancia de promover una conciencia y comportamiento seguros entre los empleados y usuarios.

5. **<u>Brechas de Seguridad</u>:**

- **¿Cómo ha impactado la configuración de identidades privilegiadas en dentro de una institución en las posibles brechas de seguridad?**

La configuración de identidades privilegiadas puede influir directamente en posibles brechas de seguridad, requiriendo medidas de respuesta y recuperación específicas.

- **¿Se ha observado algún cambio en el panorama de seguridad como resultado de estas configuraciones?**

  Observar cambios en el panorama de seguridad debido a configuraciones de identidades privilegiadas es esencial para adaptar las estrategias de ciberseguridad.

- **¿Cuáles son las medidas de respuesta y recuperación ante posibles brechas de seguridad relacionadas con identidades privilegiadas?**

La equidad en el acceso a oportunidades de desarrollo de habilidades digitales debe ser considerada al abordar brechas de seguridad relacionadas con identidades privilegiadas.

- **¿Cómo la configuración de identidades privilegiadas afecta las posibles brechas de seguridad, considerando las dinámicas socioeconómicas?**

Evaluar la capacitación continua y la concientización de los usuarios en relación con la configuración de identidades privilegiadas es esencial para prevenir posibles brechas de seguridad.

- **¿Se han implementado medidas específicas para abordar las brechas de seguridad relacionadas con la equidad en el acceso a oportunidades de desarrollo de habilidades digitales?**

La colaboración con expertos en ciberseguridad externos puede proporcionar perspectivas adicionales sobre posibles brechas

relacionadas con identidades privilegiadas y mejorar la eficacia de las medidas de respuesta y recuperación.

Sección 3: Comparación de Soluciones y Mejores Prácticas Actuales

6. **<u>Herramientas y Tecnologías</u>:**

   - **¿Cómo se consideran las habilidades digitales y la participación en la selección de herramientas y tecnologías para la gestión de identidades privilegiadas dentro de una institución?**

   Las habilidades digitales y la participación deben ser consideradas en la selección de herramientas y tecnologías para la gestión de identidades privilegiadas.

   - **¿Existe algún sesgo o desequilibrio en el acceso a estas herramientas basado en las identidades privilegiadas dentro de la institución?**

   Es importante evitar sesgos en el acceso a herramientas basado en identidades privilegiadas y abordar cualquier desafío específico al implementar tecnologías de gestión de identidades privilegiadas.

   - **¿Qué desafíos específicos se han enfrentado al implementar tecnologías de gestión de identidades privilegiadas y cómo se han abordado?**

   Las interacciones de poder y disparidades socioeconómicas deben ser tenidas en cuenta al seleccionar herramientas y tecnologías para asegurar una gestión equitativa.

   - **¿Cómo las interacciones de poder y las disparidades socioeconómicas influyen en la selección de herramientas y tecnologías para la gestión de identidades privilegiadas?**

   La evaluación constante de las necesidades de seguridad y la alineación de las herramientas y tecnologías con los objetivos institucionales son esenciales para una gestión efectiva de identidades privilegiadas.

- **¿Qué desafíos específicos se enfrentan al implementar tecnologías de gestión de identidades privilegiadas considerando estas complejas dinámicas?**

Fomentar la transparencia en el proceso de selección de herramientas y tecnologías, garantizando la participación equitativa de todos los interesados, contribuirá a evitar sesgos y promoverá un enfoque más inclusivo en la gestión de identidades privilegiadas.

7. **Mejores Prácticas Existentes:**

- **¿Cómo influyen las oportunidades de desarrollo de habilidades digitales en la adopción de mejores prácticas en la gestión de identidades privilegiadas?**

Las oportunidades de desarrollo de habilidades digitales influyen en la adopción de mejores prácticas en la gestión de identidades privilegiadas.

- **¿Se han identificado mejores prácticas específicas para mitigar riesgos asociados a identidades privilegiadas en entornos institucionales?**

Identificar e implementar mejores prácticas específicas es esencial para mitigar riesgos asociados a identidades privilegiadas.

- **¿En qué medida se han implementado y evaluado estas mejores prácticas en entornos institucionales?**

Evaluar regularmente la implementación de estas mejores prácticas en entornos institucionales es fundamental para mantener la seguridad.

Sección 4: Recomendaciones y Estrategias Efectivas

8. **Hallazgos Clave:**

- **¿Cómo afectan las habilidades digitales, la participación y la productividad en los hallazgos clave del análisis de identidades privilegiadas?**

Las habilidades digitales, la participación y la productividad influyen en los hallazgos clave del análisis de identidades privilegiadas.

- **¿Qué recomendaciones específicas se proponen para abordar las implicaciones identificadas en la ciberseguridad?**

Se proponen recomendaciones específicas para abordar las implicaciones identificadas en ciberseguridad, considerando su integración en las operaciones diarias.

- **¿Cómo se pueden integrar estas recomendaciones en las operaciones diarias?**

Las implicaciones sociales y éticas deben ser consideradas al adoptar mejores prácticas para la gestión de identidades privilegiadas.

- **¿Cómo se han considerado las implicaciones sociales y éticas en la adopción de mejores prácticas para la gestión de identidades privilegiadas?**

Se deben identificar y proponer mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder en la configuración de identidades privilegiadas.

- **¿Se han identificado mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder en la configuración de identidades privilegiadas?**

Evaluar cómo las interacciones de poder y las disparidades socioeconómicas influyen en los hallazgos clave del análisis de identidades privilegiadas es crucial para una comprensión completa de los resultados.

- **¿Cómo las complejas interacciones de poder y las disparidades socioeconómicas influyen en los hallazgos clave del análisis de identidades privilegiadas?**

Las recomendaciones específicas propuestas deben ser adaptadas a la cultura organizativa y sus características únicas para asegurar una integración efectiva en las operaciones diarias.

- **¿Qué recomendaciones específicas se proponen para abordar las implicaciones sociales y éticas identificadas en la ciberseguridad?**

Identificar y promover mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder contribuirá a un enfoque más equitativo y sostenible en la gestión de identidades privilegiadas.

9. **<u>Recomendaciones y Estrategias</u>:**

- **¿Cómo se pueden mejorar las oportunidades de desarrollo de habilidades digitales de manera equitativa para reducir la configuración de identidades privilegiadas?**

Mejorar equitativamente las oportunidades de desarrollo de habilidades digitales es esencial para reducir la configuración de identidades privilegiadas.

- **¿Qué estrategias se sugieren para abordar los riesgos tecnológicos emergentes asociados a las configuraciones de identidades privilegiadas en entornos institucionales?**

Estrategias específicas deben ser sugeridas para abordar los riesgos tecnológicos emergentes asociados a las configuraciones de identidades privilegiadas.

- **¿Qué medidas proactivas se pueden tomar para fomentar la diversidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas?**

Medidas proactivas deben ser tomadas para fomentar la diversidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas.

- **¿Cómo se pueden diseñar estrategias que aborden de manera efectiva las complejas interacciones de poder y las disparidades socioeconómicas en la gestión de identidades privilegiadas?**

Diseñar estrategias efectivas que aborden las complejas interacciones de poder y disparidades socioeconómicas en la gestión de identidades privilegiadas es crucial.

- **¿Cuáles son los pasos concretos para promover la equidad digital y reducir las desigualdades socioeconómicas en el uso de TIC?**

Establecer pasos concretos para promover la equidad digital y reducir las desigualdades socioeconómicas en el uso de TIC es fundamental para lograr una gestión justa de identidades privilegiadas.

Entrevistado número dos Especialista en Networking, Telecomunicaciones y Ciberseguridad:

Sección 1: Análisis de la Gestión de Identidades Privilegiadas en entornos institucionales

1. **Antecedentes Generales:**

   - **¿Cómo afectan las identidades privilegiadas y los riesgos emergentes en la ciberseguridad, y cuáles son las implicaciones para la protección de la información y la infraestructura digital?**

   La incidencia de identidades privilegiadas y los riesgos emergentes en ciberseguridad impactan de manera directa en la salvaguarda de la información y la infraestructura digital. Es crucial entender la naturaleza de esta influencia para fortalecer de manera efectiva la seguridad institucional.

   - **¿Cómo contribuyen estas condiciones a la configuración de identidades privilegiadas en el uso de TIC?**

   La configuración de identidades privilegiadas en el uso de TIC se ve moldeada por condiciones específicas, como los cambios en la ciberseguridad y las intrincadas interacciones entre diversos actores en el entorno digital. Estos factores colectivos influyen en la forma en que se establecen y gestionan estas identidades.

- **¿Existe alguna relación entre las identidades privilegiadas y posibles brechas de seguridad en el entorno digital?**

Existe una conexión directa entre las identidades privilegiadas y las potenciales brechas de seguridad, resaltando la necesidad apremiante de una gestión efectiva para prevenir vulnerabilidades y garantizar la integridad de la seguridad digital.

- **¿Quiénes son los actores que ostentan estas identidades privilegiadas y cómo configuran estas interacciones en el espacio digital?**

Identificar a los actores que detentan identidades privilegiadas y comprender cómo sus interacciones se manifiestan en el espacio digital es esencial para fortalecer la seguridad, abordando así las complejidades inherentes a estas configuraciones.

- **¿Cómo estas interacciones de poder se traducen en la configuración de identidades privilegiadas en el uso de TIC?**

Las interacciones de poder no solo influyen en la configuración de identidades privilegiadas en el uso de TIC, sino que también se entrelazan con la estructura organizativa y las políticas internas de la institución. Esta conexión añade capas de complejidad que deben considerarse para una gestión efectiva de identidades privilegiadas.

- **¿Existe una relación entre las disparidades socioeconómicas preexistentes y la asignación de identidades privilegiadas?**

Considerar las disparidades socioeconómicas preexistentes es esencial al analizar la asignación de identidades privilegiadas. Estas disparidades pueden influir significativamente en la configuración y gestión de identidades, impactando más allá de la seguridad informática e involucrando aspectos más amplios de la institución.

2. Prácticas Actuales:

- **¿Quiénes tienen acceso a oportunidades de desarrollo de habilidades digitales y cómo esto influye en la configuración y**

perpetuación de identidades privilegiadas en el uso y control de las TIC?

El acceso a oportunidades de desarrollo de habilidades digitales juega un papel determinante en la configuración y perpetuación de identidades privilegiadas en el control de las TIC.

- **¿Cómo estas condiciones afectan la participación y la productividad?**

La equidad en el acceso a oportunidades de desarrollo de habilidades digitales es esencial para garantizar una participación y productividad justas.

- **¿Se han implementado medidas específicas para abordar la equidad en el acceso a oportunidades de desarrollo de habilidades digitales?**

Es imperativo implementar medidas específicas que aborden la equidad en el acceso a oportunidades de desarrollo de habilidades digitales y gestionar las identidades privilegiadas de manera equitativa.

- **¿Cómo se reflejan y refuerzan las disparidades socioeconómicas preexistentes en las prácticas actuales de gestión de identidades privilegiadas?**

Identificar y abordar las disparidades socioeconómicas presentes en las prácticas actuales es crucial para lograr una gestión equitativa de identidades privilegiadas.

- **¿Qué medidas se han implementado para abordar la equidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas?**

La colaboración entre diferentes departamentos y equipos dentro de la institución puede influir en la distribución de identidades privilegiadas. Comprender cómo estas interacciones afectan la configuración actual es esencial para desarrollar estrategias de gestión más efectivas.

3. Áreas de Mejora:

- **¿Cómo la configuración actual de identidades privilegiadas dentro de una institución podría afectar la eficiencia y efectividad de las operaciones internas?**

La configuración actual de identidades privilegiadas puede impactar significativamente la eficiencia y efectividad de las operaciones internas, por lo que es crucial evaluar y mejorar estas configuraciones.

- **¿Existen áreas específicas donde se podría mejorar la gestión de identidades privilegiadas para aumentar la seguridad y eficacia operativa?**

Identificar áreas específicas para mejorar la gestión de identidades privilegiadas puede contribuir a aumentar la seguridad y eficacia operativa de la institución.

- **¿En qué medida las interacciones de poder afectan la eficiencia y efectividad de las operaciones internas?**

Es esencial considerar las interacciones de poder al evaluar la eficiencia operativa, implementando medidas para mitigar su impacto y promover un entorno más equitativo.

- **¿Cómo las disparidades socioeconómicas se traducen en desafíos específicos para la mejora de la gestión de identidades privilegiadas?**
- Abordar las disparidades socioeconómicas es fundamental para superar desafíos específicos en la mejora de la gestión de identidades privilegiadas y lograr un sistema más equitativo.

Sección 2: Evaluación de Riesgos Asociados a Identidades Privilegiadas en TIC

4. Amenazas Internas y Externas:

- **¿Cómo se relacionan las habilidades digitales, la participación y la productividad con las amenazas internas y externas asociadas a identidades privilegiadas?**

Las habilidades digitales, la participación y la productividad están intrínsecamente ligadas a las amenazas internas y externas vinculadas a identidades privilegiadas.

- **¿Existen riesgos tecnológicos emergentes asociados a estas configuraciones en entornos institucionales?**

Es crucial identificar los riesgos tecnológicos emergentes y aplicar estrategias específicas para mitigar dichas amenazas en entornos institucionales.

- **¿Se han identificado estrategias específicas para mitigar los riesgos tecnológicos emergentes relacionados con identidades privilegiadas?**

La comprensión y abordaje de las complejas interacciones de poder son esenciales para gestionar eficazmente las amenazas internas y externas ligadas a identidades privilegiadas.

- **¿Cómo las complejas interacciones de poder contribuyen a las amenazas internas y externas asociadas a identidades privilegiadas?**

Las dinámicas de poder complejas contribuyen significativamente a las amenazas internas y externas vinculadas a identidades privilegiadas, haciendo imperativo abordar y entender estas dinámicas.

- **¿Cuál es el impacto de las disparidades socioeconómicas en la gestión de riesgos tecnológicos emergentes en entornos institucionales?**

Las disparidades socioeconómicas impactan la gestión de riesgos tecnológicos emergentes, y deben ser consideradas en el desarrollo de estrategias de mitigación para garantizar una respuesta equitativa.

5. Brechas de Seguridad:

- **¿Cómo ha impactado la configuración de identidades privilegiadas dentro de una institución en las posibles brechas de seguridad?**

La configuración de identidades privilegiadas puede influir directamente en las posibles brechas de seguridad, requiriendo medidas específicas de respuesta y recuperación.

- **¿Se ha observado algún cambio en el panorama de seguridad como resultado de estas configuraciones?**

Observar cambios en el panorama de seguridad debido a las configuraciones de identidades privilegiadas es esencial para adaptar las estrategias de ciberseguridad.

- **¿Cuáles son las medidas de respuesta y recuperación ante posibles brechas de seguridad relacionadas con identidades privilegiadas?**

La equidad en el acceso a oportunidades de desarrollo de habilidades digitales debe ser un factor clave al abordar las brechas de seguridad relacionadas con identidades privilegiadas.

- **¿Cómo la configuración de identidades privilegiadas afecta las posibles brechas de seguridad, considerando las dinámicas socioeconómicas?**

Evaluar la capacitación continua y la concientización de los usuarios en relación con la configuración de identidades privilegiadas es esencial para prevenir posibles brechas de seguridad.

- **¿Se han implementado medidas específicas para abordar las brechas de seguridad relacionadas con la equidad en el acceso a oportunidades de desarrollo de habilidades digitales?**

Colaborar con expertos externos en ciberseguridad puede proporcionar perspectivas adicionales sobre posibles brechas relacionadas con identidades privilegiadas y mejorar la eficacia de las medidas de respuesta y recuperación.

Sección 3: Evaluación de Soluciones y Prácticas Existentes

6. Estrategias y Tecnologías:

- **¿Cómo afectan las habilidades digitales y la participación en la elección de estrategias y tecnologías para la gestión de identidades privilegiadas dentro de una institución?**

La elección de estrategias y tecnologías para la gestión de identidades privilegiadas debe considerar directamente las habilidades digitales y la participación.

- **¿Existe algún sesgo o desequilibrio en el acceso a estas herramientas basado en las identidades privilegiadas dentro de la institución?**

Es crucial evitar cualquier sesgo en el acceso a herramientas basado en identidades privilegiadas y abordar desafíos específicos al implementar tecnologías de gestión de identidades privilegiadas.

- **¿Cuáles son los desafíos específicos encontrados al implementar tecnologías de gestión de identidades privilegiadas y cómo se han abordado?**

Las interacciones de poder y disparidades socioeconómicas deben tenerse en cuenta al seleccionar estrategias y tecnologías para garantizar una gestión justa.

- **¿Cómo influyen las interacciones de poder y las disparidades socioeconómicas en la elección de estrategias y tecnologías para la gestión de identidades privilegiadas?**

Evaluar continuamente las necesidades de seguridad y alinear estrategias y tecnologías con los objetivos institucionales son esenciales para una gestión efectiva de identidades privilegiadas.

- **¿Qué desafíos específicos se enfrentan al implementar tecnologías de gestión de identidades privilegiadas considerando estas complejas dinámicas?**

Promover la transparencia en el proceso de selección de estrategias y tecnologías, garantizando la participación equitativa de todos los interesados,

contribuirá a evitar sesgos y promoverá un enfoque más inclusivo en la gestión de identidades privilegiadas.

7. Mejores Prácticas Actuales:

- **¿Cómo afectan las oportunidades de desarrollo de habilidades digitales en la adopción de mejores prácticas en la gestión de identidades privilegiadas?**

Las oportunidades de desarrollo de habilidades digitales tienen un impacto positivo en la adopción de mejores prácticas en la gestión de identidades privilegiadas.

- **¿Se han identificado mejores prácticas específicas para mitigar riesgos asociados a identidades privilegiadas en entornos institucionales?**

Identificar e implementar prácticas efectivas es esencial para mitigar los riesgos asociados a identidades privilegiadas.

- **¿En qué medida se han implementado y evaluado estas mejores prácticas en entornos institucionales?**

Evaluar de manera regular la implementación de estas mejores prácticas en entornos institucionales es fundamental para garantizar y mejorar la seguridad.

Sección 4: Sugerencias y Estrategias Efectivas

8. Puntos Destacados:

- **¿Cómo influyen las habilidades digitales, la participación y la productividad en los puntos destacados del análisis de identidades privilegiadas?**

Las habilidades digitales, la participación y la productividad desempeñan un papel significativo en los puntos destacados del análisis de identidades privilegiadas.

- **¿Qué recomendaciones específicas se proponen para abordar las implicaciones identificadas en ciberseguridad?**

Se proponen recomendaciones concretas para abordar las implicaciones identificadas en ciberseguridad, asegurando su integración efectiva en las operaciones diarias.

- **¿Cómo se pueden integrar estas recomendaciones en las operaciones diarias?**

La integración de estas recomendaciones en las operaciones diarias debe considerar las implicaciones sociales y éticas.

- **¿Cómo se han considerado las implicaciones sociales y éticas en la adopción de mejores prácticas para la gestión de identidades privilegiadas?**

Identificar y proponer mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder en la configuración de identidades privilegiadas es fundamental.

- **¿Se han identificado mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder en la configuración de identidades privilegiadas?**

Evaluar cómo las interacciones de poder y las disparidades socioeconómicas influyen en los puntos destacados del análisis de identidades privilegiadas es crucial para comprender completamente los resultados.

- **¿Cómo las complejas interacciones de poder y las disparidades socioeconómicas influyen en los puntos destacados del análisis de identidades privilegiadas?**

Las recomendaciones específicas propuestas deben adaptarse a la cultura organizativa y sus características únicas para garantizar una integración efectiva en las operaciones diarias.

- **¿Qué recomendaciones específicas se proponen para abordar las implicaciones sociales y éticas identificadas en ciberseguridad?**

Identificar y promover mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder contribuirá a un

enfoque más equitativo y sostenible en la gestión de identidades privilegiadas.

9. Recomendaciones y Estrategias:

- **¿Cómo se pueden mejorar las oportunidades de desarrollo de habilidades digitales de manera equitativa para reducir la configuración de identidades privilegiadas?**

Mejorar de manera equitativa las oportunidades de desarrollo de habilidades digitales es esencial para reducir la configuración de identidades privilegiadas.

- **¿Qué estrategias se sugieren para abordar los riesgos tecnológicos emergentes asociados a las configuraciones de identidades privilegiadas en entornos institucionales?**

Estrategias específicas deben ser sugeridas para abordar los riesgos tecnológicos emergentes asociados a las configuraciones de identidades privilegiadas.

- **¿Qué medidas proactivas se pueden tomar para fomentar la diversidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas?**

Tomar medidas proactivas para fomentar la diversidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas es esencial.

- **¿Cómo se pueden diseñar estrategias que aborden de manera efectiva las complejas interacciones de poder y las disparidades socioeconómicas en la gestión de identidades privilegiadas?**

Diseñar estrategias efectivas que aborden las complejas interacciones de poder y disparidades socioeconómicas en la gestión de identidades privilegiadas es crucial.

- **¿Cuáles son los pasos concretos para promover la equidad digital y reducir las desigualdades socioeconómicas en el uso de TIC?**

Establecer pasos concretos para promover la equidad digital y reducir las desigualdades socioeconómicas en el uso de TIC es fundamental para lograr una gestión justa de identidades privilegiadas.

Entrevistado número tres Especialista en Desarrollo Informático y Ciberseguridad:

Sección 1: Análisis de la Gestión de Identidades Privilegiadas en entornos institucionales

1. Antecedentes Generales:

- **¿Cómo afectan las identidades privilegiadas y los riesgos emergentes en la ciberseguridad, y cuáles son las implicaciones para la protección de la información y la infraestructura digital?**

Las implicaciones de las identidades privilegiadas y los riesgos emergentes en ciberseguridad repercuten directamente en la salvaguarda de la información y la infraestructura digital. Entender a fondo estas dinámicas es esencial para robustecer la seguridad institucional y prevenir posibles amenazas.

- **¿Cómo contribuyen estas condiciones a la configuración de identidades privilegiadas en el uso de TIC?**

Las condiciones cambiantes de ciberseguridad y las complejas interacciones entre actores diversos en el entorno digital son factores determinantes en la configuración de identidades privilegiadas en el uso de TIC. Estos elementos colectivos influyen de manera integral en la forma en que se establecen y gestionan dichas identidades.

- **¿Existe alguna relación entre las identidades privilegiadas y posibles brechas de seguridad en el entorno digital?**

La conexión directa entre identidades privilegiadas y posibles brechas de seguridad subraya la importancia crítica de gestionar estas identidades de manera eficaz. Es esencial para prevenir vulnerabilidades y mantener la integridad de la seguridad digital de la institución.

- **¿Quiénes son los actores que ostentan estas identidades privilegiadas y cómo configuran estas interacciones en el espacio digital?**

Identificar a los actores que ostentan identidades privilegiadas y comprender cómo sus interacciones se reflejan en el espacio digital son aspectos fundamentales para fortalecer la seguridad. Esto implica abordar las complejidades inherentes a la configuración de estas identidades desde una perspectiva amplia.

- **¿Cómo estas interacciones de poder se traducen en la configuración de identidades privilegiadas en el uso de TIC?**

Las interacciones de poder no solo influyen en la configuración de identidades privilegiadas en el uso de TIC, sino que también se entrelazan con la estructura organizativa y las políticas internas de la institución. Este entrelazamiento añade capas de complejidad que deben considerarse para una gestión completa y efectiva de identidades privilegiadas.

- **¿Existe una relación entre las disparidades socioeconómicas preexistentes y la asignación de identidades privilegiadas?**

Considerar las disparidades socioeconómicas preexistentes es esencial al analizar la asignación de identidades privilegiadas. Estas disparidades pueden influir de manera significativa en la configuración y gestión de identidades, afectando no solo la seguridad informática, sino también aspectos más amplios de la institución, como la confianza de los usuarios y la reputación institucional.

2. Prácticas Actuales:

- **¿Quiénes tienen acceso a oportunidades de desarrollo de habilidades digitales y cómo esto influye en la configuración y perpetuación de identidades privilegiadas en el uso y control de las TIC?**

El acceso equitativo a oportunidades de desarrollo de habilidades digitales es esencial para desafiar y superar la configuración de identidades privilegiadas en el control de las TIC.

- **¿Cómo estas condiciones afectan la participación y la productividad?**

La igualdad de acceso a oportunidades de desarrollo de habilidades digitales es un factor clave para garantizar una participación y productividad justas en el entorno digital.

- **¿Se han implementado medidas específicas para abordar la equidad en el acceso a oportunidades de desarrollo de habilidades digitales?**

Es crucial implementar medidas específicas que promuevan la equidad en el acceso a oportunidades de desarrollo de habilidades digitales y gestionen de manera justa las identidades privilegiadas.

- **¿Cómo se reflejan y refuerzan las disparidades socioeconómicas preexistentes en las prácticas actuales de gestión de identidades privilegiadas?**

Identificar y abordar las disparidades socioeconómicas presentes en las prácticas actuales es esencial para lograr una gestión equitativa de identidades privilegiadas.

- **¿Qué medidas se han implementado para abordar la equidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas?**

La colaboración entre diferentes departamentos y equipos dentro de la institución puede influir en la distribución equitativa de identidades privilegiadas. Comprender cómo estas interacciones afectan la configuración actual es esencial para desarrollar estrategias de gestión más efectivas.

3. Áreas de Mejora:

- **¿Cómo la configuración actual de identidades privilegiadas dentro de una institución podría afectar la eficiencia y efectividad de las operaciones internas?**

La configuración actual de identidades privilegiadas puede tener un impacto significativo en la eficiencia y efectividad de las operaciones internas, por lo que es crucial evaluar y mejorar estas configuraciones.

- **¿Existen áreas específicas donde se podría mejorar la gestión de identidades privilegiadas para aumentar la seguridad y eficacia operativa?**

Identificar áreas específicas para mejorar la gestión de identidades privilegiadas puede contribuir a aumentar la seguridad y eficacia operativa de la institución.

- **¿En qué medida las interacciones de poder afectan la eficiencia y efectividad de las operaciones internas?**

Es esencial considerar las interacciones de poder al evaluar la eficiencia operativa, implementando medidas para mitigar su impacto y promover un entorno más equitativo.

- **¿Cómo las disparidades socioeconómicas se traducen en desafíos específicos para la mejora de la gestión de identidades privilegiadas?**

Abordar las disparidades socioeconómicas es fundamental para superar desafíos específicos en la mejora de la gestión de identidades privilegiadas y lograr un sistema más equitativo.

Sección 2: Evaluación de Riesgos Asociados a Identidades Privilegiadas en TIC 4. Amenazas Internas y Externas:

- **¿Cómo se relacionan las habilidades digitales, la participación y la productividad con las amenazas internas y externas asociadas a identidades privilegiadas?**

Las habilidades digitales, la participación y la productividad están intrínsecamente ligadas a las amenazas internas y externas vinculadas a identidades privilegiadas.

- **¿Existen riesgos tecnológicos emergentes asociados a estas configuraciones en entornos institucionales?**

Es crucial identificar los riesgos tecnológicos emergentes y aplicar estrategias específicas para mitigar dichas amenazas en entornos institucionales.

- **¿Se han identificado estrategias específicas para mitigar los riesgos tecnológicos emergentes relacionados con identidades privilegiadas?**

La comprensión y abordaje de las complejas interacciones de poder son esenciales para gestionar eficazmente las amenazas internas y externas ligadas a identidades privilegiadas.

- **¿Cómo las complejas interacciones de poder contribuyen a las amenazas internas y externas asociadas a identidades privilegiadas?**

Las dinámicas de poder complejas contribuyen significativamente a las amenazas internas y externas vinculadas a identidades privilegiadas, haciendo imperativo abordar y entender estas dinámicas.

- **¿Cuál es el impacto de las disparidades socioeconómicas en la gestión de riesgos tecnológicos emergentes en entornos institucionales?**

Las disparidades socioeconómicas impactan la gestión de riesgos tecnológicos emergentes, y deben ser consideradas en el desarrollo de estrategias de mitigación para garantizar una respuesta equitativa.

5. Brechas de Seguridad:

- **¿Cómo ha impactado la configuración de identidades privilegiadas dentro de una institución en las posibles brechas de seguridad?**

La configuración de identidades privilegiadas puede influir directamente en las posibles brechas de seguridad, requiriendo medidas específicas de respuesta y recuperación.

- **¿Se ha observado algún cambio en el panorama de seguridad como resultado de estas configuraciones?**

Observar cambios en el panorama de seguridad debido a las configuraciones de identidades privilegiadas es esencial para adaptar las estrategias de ciberseguridad.

- **¿Cuáles son las medidas de respuesta y recuperación ante posibles brechas de seguridad relacionadas con identidades privilegiadas?**

La equidad en el acceso a oportunidades de desarrollo de habilidades digitales debe ser un factor clave al abordar las brechas de seguridad relacionadas con identidades privilegiadas.

- **¿Cómo la configuración de identidades privilegiadas afecta las posibles brechas de seguridad, considerando las dinámicas socioeconómicas?**

Evaluar la capacitación continua y la concientización de los usuarios en relación con la configuración de identidades privilegiadas es esencial para prevenir posibles brechas de seguridad.

- **¿Se han implementado medidas específicas para abordar las brechas de seguridad relacionadas con la equidad en el acceso a oportunidades de desarrollo de habilidades digitales?**

Colaborar con expertos externos en ciberseguridad puede proporcionar perspectivas adicionales sobre posibles brechas relacionadas con identidades privilegiadas y mejorar la eficacia de las medidas de respuesta y recuperación.

Sección 3: Evaluación de Soluciones y Prácticas Existentes

6. **Estrategias y Tecnologías:**

- **¿Cómo afectan las habilidades digitales y la participación en la elección de estrategias y tecnologías para la gestión de identidades privilegiadas dentro de una institución?**

La elección de estrategias y tecnologías para la gestión de identidades privilegiadas debe considerar directamente las habilidades digitales y la participación de manera equitativa.

- **¿Existe algún sesgo o desequilibrio en el acceso a estas herramientas basado en las identidades privilegiadas dentro de la institución?**

Es crucial evitar cualquier sesgo en el acceso a herramientas basado en identidades privilegiadas y abordar desafíos específicos al implementar tecnologías de gestión de identidades privilegiadas.

- **¿Cuáles son los desafíos específicos encontrados al implementar tecnologías de gestión de identidades privilegiadas y cómo se han abordado?**

Las interacciones de poder y disparidades socioeconómicas deben tenerse en cuenta al seleccionar estrategias y tecnologías para garantizar una gestión justa.

- **¿Cómo influyen las interacciones de poder y las disparidades socioeconómicas en la elección de estrategias y tecnologías para la gestión de identidades privilegiadas?**

Evaluar continuamente las necesidades de seguridad y alinear estrategias y tecnologías con los objetivos institucionales son esenciales para una gestión efectiva de identidades privilegiadas.

- **¿Qué desafíos específicos se enfrentan al implementar tecnologías de gestión de identidades privilegiadas considerando estas complejas dinámicas?**

Promover la transparencia en el proceso de selección de estrategias y tecnologías, garantizando la participación equitativa de todos los interesados, contribuirá a evitar sesgos y promoverá un enfoque más inclusivo en la gestión de identidades privilegiadas.

7. **Mejores Prácticas Actuales:**

- **¿Cómo afectan las oportunidades de desarrollo de habilidades digitales en la adopción de mejores prácticas en la gestión de identidades privilegiadas?**

Las oportunidades de desarrollo de habilidades digitales tienen un impacto positivo en la adopción de mejores prácticas en la gestión de identidades privilegiadas.

- **¿Se han identificado mejores prácticas específicas para mitigar riesgos asociados a identidades privilegiadas en entornos institucionales?**

Identificar e implementar prácticas efectivas es esencial para mitigar los riesgos asociados a identidades privilegiadas.

- **¿En qué medida se han implementado y evaluado estas mejores prácticas en entornos institucionales?**

Evaluar de manera regular la implementación de estas mejores prácticas en entornos institucionales es fundamental para garantizar y mejorar la seguridad.

Sección 4: Sugerencias y Estrategias Efectivas

Puntos Destacados:

- **¿Cómo influyen las habilidades digitales, la participación y la productividad en los puntos destacados del análisis de identidades privilegiadas?**

Las habilidades digitales, la participación y la productividad desempeñan un papel significativo en los puntos destacados del análisis de identidades privilegiadas.

- **¿Qué recomendaciones específicas se proponen para abordar las implicaciones identificadas en ciberseguridad?**

Se proponen recomendaciones concretas para abordar las implicaciones identificadas en ciberseguridad, asegurando su integración efectiva en las operaciones diarias.

- **¿Cómo se pueden integrar estas recomendaciones en las operaciones diarias?**

La integración de estas recomendaciones en las operaciones diarias debe considerar las implicaciones sociales y éticas.

- **¿Cómo se han considerado las implicaciones sociales y éticas en la adopción de mejores prácticas para la gestión de identidades privilegiadas?**

Identificar y proponer mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder en la configuración de identidades privilegiadas es fundamental.

- **¿Se han identificado mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder en la configuración de identidades privilegiadas?**

Evaluar cómo las interacciones de poder y las disparidades socioeconómicas influyen en los puntos destacados del análisis de identidades privilegiadas es crucial para comprender completamente los resultados.

- **¿Cómo las complejas interacciones de poder y las disparidades socioeconómicas influyen en los puntos destacados del análisis de identidades privilegiadas?**

Las recomendaciones específicas propuestas deben adaptarse a la cultura organizativa y sus características únicas para garantizar una integración efectiva en las operaciones diarias.

- **¿Qué recomendaciones específicas se proponen para abordar las implicaciones sociales y éticas identificadas en ciberseguridad?**

Identificar y promover mejores prácticas específicas para abordar las desigualdades socioeconómicas y las interacciones de poder contribuirá a un enfoque más equitativo y sostenible en la gestión de identidades privilegiadas.

9. **Recomendaciones y Estrategias:**

- **¿Cómo se pueden mejorar las oportunidades de desarrollo de habilidades digitales de manera equitativa para reducir la configuración de identidades privilegiadas?**

Mejorar de manera equitativa las oportunidades de desarrollo de habilidades digitales es esencial para reducir la configuración de identidades privilegiadas.

- **¿Qué estrategias se sugieren para abordar los riesgos tecnológicos emergentes asociados a las configuraciones de identidades privilegiadas en entornos institucionales?**

Estrategias específicas deben ser sugeridas para abordar los riesgos tecnológicos emergentes asociados a las configuraciones de identidades privilegiadas.

- **¿Qué medidas proactivas se pueden tomar para fomentar la diversidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas?**

Tomar medidas proactivas para fomentar la diversidad en el acceso a oportunidades de desarrollo de habilidades digitales y la gestión de identidades privilegiadas es esencial.

- **¿Cómo se pueden diseñar estrategias que aborden de manera efectiva las complejas interacciones de poder y las disparidades socioeconómicas en la gestión de identidades privilegiadas?**

Diseñar estrategias efectivas que aborden las complejas interacciones de poder y disparidades socioeconómicas en la gestión de identidades privilegiadas es crucial.

- **¿Cuáles son los pasos concretos para promover la equidad digital y reducir las desigualdades socioeconómicas en el uso de TIC?**

Establecer pasos concretos para promover la equidad digital y reducir las desigualdades socioeconómicas en el uso de TIC es fundamental para lograr una gestión justa de identidades privilegiadas.