Seminario de Seguridad, Escuela Colombiana de Ingeniería Julio Garavito - Administración de Acceso Privilegiado

Angie Daniela Ruiz Alfonso
Ingeniería de Sistemas
Escuela Colombiana de Ingeniería Julio 10 Garavito
Bogotá, Colombia
angie.ruiz@mail.escuelaing.edu.co

Carlos Andrés Amorocho Amorocho
Ingeniería de Sistemas
Escuela Colombiana de Ingeniería Julio Garavito
Bogotá, Colombia
carlos.amorocho@mail.escuelaing.edu.co

***Abstract*—Privileged Access Administration, Privileged Account, Principle of Least Privilege, PASM, PEDM, Industry 4.0, Information Security.**

This article we introduces to Privileged Access Administration (PAM), first deepening in its importance and its latest technological trends implemented. After that, the main concept is found in a clearer and more specific way, what needs it solves, how it has helped society over time, its relationship with Information Security, its advantages and disadvantages.

Then there are exposed the best practices, the current leaders in the industry, the attacks on active directories and the different PAM tools investigated. To finally, describe the final architecture of the practical part of this investigation, with the documentation of the results obtained and their respective conclusions.

I. Introducción

En los últimos años, el concepto Industria 4.0 ha tomado fuerza, este se refiere a la nueva era en la que se combinan técnicas avanzadas de producción y operaciones con diferentes tecnologías. Para esto, las organizaciones deben identificar herramientas tecnológicas que satisfagan sus necesidades, con el fin de automatizar al máximo sus procesos, almacenando toda la información en formato digital, logrando garantizar de esta manera un ciclo continuo del negocio, debido a que se tiene acceso a la información en tiempo real y desde diferentes localizaciones, lo que también permite tener una mayor conectividad entre industrias.

En los últimos años el concepto Industria 4.0 ha tomado fuerza, este se refiere a la nueva era en la que se combinan técnicas avanzadas de producción y operaciones con diferentes tecnologías. Para esto, las organizaciones deben identificar herramientas tecnológicas que satisfagan sus necesidades, con el fin de automatizar al máximo sus procesos, almacenando toda la información en formato digital, logrando garantizar así un ciclo continuo del negocio ya que se tiene acceso a la información en tiempo real y desde diferentes localizaciones, lo que también permite tener una mayor conectividad entre industrias.

Como resultado de este cambio aparece el concepto de La Administración de Acceso Privilegiado, mejor conocido como PAM, el cual es un Control crítico y estricto de Seguridad Informática, que permite a las organizaciones simplificar la forma en que definen, monitorean y administran el acceso privilegiado en sus Sistemas, Aplicaciones e Infraestructura de Tecnología de la Información (TI) [1], con el fin de lograr que siempre que una persona acceda a un Sistema con su cuenta, cumpla con el Principio del Mínimo Privilegio, lo cual quiere decir que solo se le darán a dicha persona los privilegios que estrictamente necesite para su trabajo y solamente durante el horario que tenga asignado. [2]

En este artículo profundizaremos sobre la importancia de las herramientas PAM, abordando este concepto principal de modo más concreto, junto con las necesidades que resuelve, cómo ha ayudado a la humanidad a través del tiempo, su relación con la Seguridad de la Información, sus ventajas y desventajas. Luego se expondrán las mejores prácticas, los líderes actuales de la industria, los ataques a directorios activos y las diferentes herramientas investigadas. Para finalmente describir la arquitectura propuesta como parte de un experimento práctico de esta investigación, la documentación de los resultados obtenidos y sus respectivas conclusiones.

II. Marco Teórico

La complejidad en la Gestión del Control de Acceso en las organizaciones impide que se manejen eficientemente los accesos privilegiados en los Sistemas de Información, facilitando así la acumulación de derechos elevados innecesarios, herencia de privilegios por encadenamiento de grupos, falta

de personal con dedicación completa, por ende, se generan vulnerabilidades que son utilizadas por los ciberdelincuentes, generando posibles interrupciones en la continuidad del negocio, como lo son el daño o perdida de datos valiosos y/o sensibles, y es allí, donde la Administración de Acceso Privilegiado deja de ser opcional y se convierte en vital para las compañías en sus operaciones. [1]

Al contar con un Control total sobre las cuentas del Sistema se previenen futuros ataques que puedan violar la Integridad, Confidencialidad y Disponibilidad de la información. Las soluciones PAM, son capaces de reducir o eliminar la necesidad de compartir las contraseñas por medio de controles técnicos que restringen el acceso a los usuarios no autorizados. [2]

III. Administración del Acceso Privilegiado

La Administración de Acceso Privilegiado (PAM) controla el acceso a las cuentas de administrador, las cuales tienen bastante poder sobre los Sistemas, Servicios y Dispositivos de toda organización, al igual que permiten ejecutar Aplicaciones o Transacciones, brindándoles así la posibilidad a los ciberdelincuentes de realizar cambios sustanciales en los Sistemas, logrando acceder a datos e IPs corporativas o robar información de identificación personal, entre otros; por ende, cuando las cuentas privilegiadas no se administran, todos los Sistemas de Tecnología de la Información (TI) y Ciberseguridad de los que depende la empresa estarán en riesgo. [2]

Además de que todas las organizaciones están sujetas a regulaciones, como lo son GDPR, PCI DSS o Sarbanes-Oxley, la Comisión de Regulaciones de Energía Federal y de América del Norte (FERC / NERC), HIPAA 2, regulaciones de nivel como la Ley de Práctica de la Información de California y la ley de privacidad de Massachusetts 201CMR17. Y se debe tener en cuenta que algunas organizaciones desean implementar las mejores prácticas como lo son Cyber Essentials o ISO 27001, donde cada uno de esos estándares mencionados anteriormente tienen el requisito de administrar el acceso privilegiado. [2]

A las organizaciones que tienen poco o ningún Control de seguimiento se les dificulta la administración de las cuentas con privilegios, además de que la mayoría de las personas piensan que los atacantes son personas externas, pero una gran fuente de los ataques proviene desde dentro de una organización. Por ello, se usan los softwares PAM, los cuales centralizan la administración de los perfiles de administrador y garantizan que se aplique el principio del mínimo privilegio, eliminando el uso compartido de contraseñas privilegiadas. [1]

Tipos de cuentas:

- **Cuentas de administrador local.**
- **Cuentas de usuarios privilegiados.**
- **Cuentas de administrador de dominio.**
- **Cuentas de usuario de emergencia.**
- **Cuentas de servicio.**
- **Cuentas de aplicación.**
- **Administradores de sombra en la nube.**
- **Usuario empresarial privilegiado.**
- **Cuentas de bot de automatización de procesos.**
- **Secure Socket Shell.**
- **Claves SSH.**
- **Secretos.**

Considerando todos los trabajos que ahora son manejados por procesos automatizados en lugar del personal de la compañía, se pueden encontrar estas cuentas en:

- **Nube (consolas en la Nube, Aplicaciones creadas con herramientas DevOps y metodologías).**
- **Centros de Datos, Aplicaciones, Servidores, Dispositivos de Red y otra infraestructura.**
- **Endpoints (iPhones, Laptops, Tablets, entre otros).**
- **Internet de las cosas (Dispositivos conectados como cámaras de video, realidad aumentada y otros Dispositivos inteligentes).**
- **Sistemas de Control industrial que permiten a los operadores monitorear y controlar los procesos industriales (petróleo y gas, servicios públicos, fabricación, productos químicos, entre otros).**

A medida que la Gestión de acceso privilegiado ha evolucionado, Gartner ha establecido dos clasificaciones para destacar las diferentes soluciones PAM, ambas soluciones tienen los mismos objetivos, pero tienen diferentes mecanismos sobre cómo se protege y se accede a la cuenta de destino: [1]

- **PASM:** Se conocen como "bóveda de contraseñas" porque cuando los usuarios necesitan acceso a un servidor específico, solicitan acceso desde la bóveda y se les otorga una cuenta con privilegios administrativos completos, cuenta que es temporal y solo es válida para una sesión, la cual se supervisa y registra. [1]

- **PEDM:** Consiste en distribuir los privilegios de acceso según los roles laborales, no se utilizan cuentas con privilegios temporales, sino que son las herramientas PEDM las que definen y asignan privilegios permanentes a las cuentas estándar. [1]

IV. Mejores Prácticas

Se debe tener en cuenta que los permisos de acceso determinan la posibilidad de que un usuario realice una acción específica o su acceso a un objeto o función, y los permisos de un usuario específico son una combinación de permisos para dicho usuario y los permisos de los grupos y roles a los que pertenece el usuario como miembro. Pero que cuando un usuario es miembro de más de un grupo o rol, los permisos denegados para un grupo o rol tienen prioridad sobre los permisos concedidos para un grupo o rol diferente. [3]

Para administrar de manera eficaz y eficiente las cuentas con privilegios, se recomienda:

- **Centralizar la administración de cuentas de usuario en todos los servidores reales y virtuales:** Se debe monitorear y auditar qué usuarios tienen acceso a cuáles máquinas. [1]

- **Integrar directorios corporativos existentes:** Se deben integrar sin problemas los múltiples directorios corporativos y Sistemas de administración de identidad, lo cual quiere decir que las identidades de grupo y equipo se asocian automáticamente a los Sistemas, Aplicaciones y Datos. [1]

- **Garantizar la autenticación contextual:** Se debe contar con autenticación de múltiples factores a servidores y roles particulares en la organización. [1]

- **Hacer cumplir el registro seguro de pulsaciones de teclas:** Las sesiones sensibles deben cumplir el registro de pulsaciones de teclas completo, de modo que las actividades del administrador se puedan rastrear en detalle. [1]

- **Implementar un Control de acceso granular:** Los usuarios pueden tener permisos de Lectura, Ejecución, Escritura, y Completo para los elementos de un Sistema, estos permisos representan las combinaciones de permisos más granulares, por ende, se deben implementar controles de grano fino para controlar quién, cuándo, cómo y desde dónde accede. [3]

- **Principio de Mínimo Privilegio:** Es necesario que una acción dentro del Sistema por un usuario tenga la cantidad requerida de permisos y no excedan este límite, para prevenir potenciales riesgos. [2]

- **Consolidar el registro de auditoría:** Se debe tener el registro de auditoría centralizado, consolidado y a detalle, de las actividades de todos los usuarios. [1]

V. Lideres de la Industria

En la figura 1 vemos el Cuadrante Mágico de Gartner, el cual es una herramienta con la cual sabemos en qué punto de innovación y nivel de desarrollo están las empresas dedicadas a la tecnología en el mercado PAM a nivel mundial. [4]

Fig. 1. Cuadrante Mágico de Gartner

A continuación, nos enfocaremos en cada líder y el porqué de su sobresalir:

- **CyberArk:** El líder de este Cuadrante Mágico es la marca PAM más grande de todas, la primera en ofrecer innovaciones al mercado. Cuenta con la mayor participación en este mercado, una larga trayectoria en este sector, un amplio alcance geográfico, sus productos reciben puntuaciones constantemente altas en las evaluaciones técnicas de Gartner al ser capaces de admitir casos de

uso complejos, tienen planeado desarrollar nuevas capacidades para extender los métodos de acceso Just-In-Time a máquinas virtuales y Servicios en la Nube, y nuevas funciones para controlar y monitorear el acceso a las Aplicaciones Web. [5]

Su producto "Privileged Access Manager" ofrece capacidades PASM como Software o SaaS. Para PEDM ofrece "Endpoint Privilege Manager" como SaaS para Windows y Mac, y "On-Demand Privileges Manager" para UNIX y Linux como Software. La gestión de Secretos la realizan a través de un producto de Software llamado "Secrets Manager", que incluye tecnología adquirida de Conjur. Pero sus productos se encuentran entre los más caros del mercado, y además, han discontinuado la versión de software de su producto Windows "Endpoint Privilege Manager", lo que obliga a todos los clientes a suscribirse a un modelo SaaS con el paso del tiempo. [5]

Sus clientes mencionan la dificultad de uso e implementación de la versión de software del producto, hasta el punto de informar que incluso las actualizaciones a menudo requieren servicios profesionales, su recuperación ante desastres es frágil al basarse en procesos manuales y las capacidades de puente de directorios y PEDM para UNIX y Linux son inferiores a las de sus principales competidores. [5]

Una de sus fortalezas, es que, en la actualidad, es el único proveedor de PAM que ofrece la funcionalidad CIEM (Gestión de derechos de infraestructura en la Nube) y al contar con un gran ecosistema de socios, ha entregado muchos conectores e integraciones con tecnologías adyacentes, como ITSM (Gestión de servicios de tecnología de la información) y herramientas de administración y gobernanza de identidad (IGA). [5]

- **BeyondTrust:** Ofrece capacidades PASM dentro de su oferta "Password Safe" como Software, Dispositivo físico/virtual, o como SaaS, y un producto de gestión de Secretos "DevOps Secrets Safe" como Software. Además, están trabajando para agregar funciones de administración de derechos de infraestructura en la Nube. [5]

  Una de sus fortalezas es el descubrimiento de cuentas, debido a que tienen un complemento que se encarga de ello y viene incluido con sus productos PAM. "Privilege Management" es la mejor oferta de su clase para UNIX y Linux PEDM, además sus controles de aplicaciones para Windows son muy sólidos y para Mac proporciona un conjunto completo de controles de aplicaciones. Cuentan con la funcionalidad de tener informes con plantillas pre configuradas personalizables, paneles de visualización y sus operaciones están diversificadas geográficamente. [5]

  Pero no han logrado cumplir con la intención de fusionar la funcionalidad de sus productos después de más de dos años, imponen un límite en la cantidad de Sistemas de destino para el modelo de licencia por usuario y la tasa de adopción de "Password Safe" en el mercado se quedó atrás, debido a que es débil en términos de administración de cuentas de Servicio y carece de un SDK que los clientes puedan usar para crear conectores personalizados para la rotación de contraseñas. [5]

- **Centrify:** Su producto "Centrify Privileged Access Service" está disponible como SaaS y se centra en PASM, mientras que "Centrify Privilege Elevation Service" tiene capacidades PEDM, antes estaba tradicionalmente centrado en directorios activos, pero su tecnología ahora se puede utilizar con otros servidores de directorio y sus operaciones se centran en América y Europa. [5]

  Una de sus fortalezas es contar con la mejor capacidad de puente de directorio para UNIX y Linux, al adaptarse a configuraciones de directorios activos complejas, la experiencia del cliente es muy buena debido a que cuentan con amplios programas de soporte, capacitación y todos los manuales son accesibles en línea sin necesidad de registrarse, ofrecen API maduras y tiene muchas integraciones listas para usar con otras herramientas de Seguridad, así como con DevOps, RPA (automatización robótica de procesos) y herramientas de administración de servicios de TI, además cuentan con una función segura llamada "Delegated Machine Credentials" que simplifica el proceso de autenticación de las identidades de máquina, sin necesidad de que las aplicaciones accedan directamente a las credenciales de texto sin cifrar. [5]

  Pero sus capacidades de gestión de cuentas de servicio y descubrimiento de cuentas privilegiadas son básicas, no ofrecen compatibilidad con PEDM para macOS, ni el Sandboxing (aislamiento de procesos) es compatible con las aplicaciones de Windows, tienen el menor personal en comparación con los demás miembros del cuadrante y a principios del presente año, la compañía fue adquirida por TPG, una firma de capital privado, y anunció una fusión con Thycotic. [5]

- **Thycotic:** Su producto "Secret Server" se centra en las capacidades de PASM y está disponible como software o SaaS. Además, ofrece capacidades PEDM para Windows, Linux y macOS, y administración de Secretos como SaaS con "DevOps Secrets Vault". [5]

  Sus fortalezas son que a diferencia de la mayoría de los otros proveedores ofrecen una gestión profunda del ciclo de vida de la identidad para las cuentas de Servicio, aunque esto requiere la compra de una herramienta separada "Thycotic Account Lifecycle Manager", son uno de los proveedores de más rápido crecimiento, sus operaciones están diversificadas geográficamente, tuvieron innovación al incluir la reparación automática de eventos definidos (como la alerta y la desactivación automática de los usuarios que han obtenido derechos de administrador fuera del Sistema PAM), la grabación de sesiones web y la extensión de sus capacidades de gestión de Secretos, además de la venta de productos complementarios para ampliar los controles de acceso privilegiado a consolas web y bases de datos con amplias capacidades de filtrado. [5]

  Pero sus precios están entre los más altos, tienen un límite estricto de 10,000 Secretos, independientemente del número de usuarios con licencia y la capacidad adicional para los Secretos requiere un pago adicional, no ofrecen monitoreo de integridad de archivos, dependen de las secuencias de comandos debido a que permite que los clientes desarrollen, o paguen a los servicios profesionales de la compañía para desarrollar capacidades a través de personalizaciones que otros proveedores ofrecen listas para usar y a principios del presente año, la compañía fue adquirida por TPG, una firma de capital privado, y anunció una fusión con Centrify. [5]

- **ARCON:** Su producto "Privileged Access Management" es entregado como un Dispositivo, Software o SaaS, el cual proporciona capacidades de almacenamiento y PASM, funcionalidad PEDM para Windows, UNIX/Linux y administración de Secretos. [5]

  Sus fortalezas son la innovación porque buscan cerrar la brecha con otros proveedores al admitir Internet de las cosas (IoT) y tecnología operativa (OT), su soporte es de 24 horas los 7 días de la semana, en la mayoría de los casos el precio del software tiene un precio inferior al promedio de la industria y la experiencia del cliente es positiva por la facilidad de integración del producto y las funcionalidades de implementación rápida que tienen. [5]

  Pero poseen una interfaz web que requiere un ActiveX o un complemento Java obsoleto en caso de que los usuarios prefieran no utilizar las herramientas cliente que ellos proporcionan, en la mayoría de los casos sus precios están por encima del promedio para la oferta de SaaS, ellos dependen principalmente del desarrollo de integración de sus clientes en otros Sistemas adyacentes a través de sus API, en lugar de ofrecer integraciones prefabricadas como parte de su producto y sus operaciones se encuentran principalmente en Asia/Pacífico y EMEA. [5]

VI. Ataques a Directorios Activos

La función de un directorio activo es proporcionar un servicio ubicado en uno o varios servidores capaz de crear objetos como usuarios, equipos o grupos para administrar las credenciales durante el inicio de sesión de los equipos que se conectan a una red. Además, permite administrar las políticas de toda la red en la que se encuentre este servidor. Está principalmente orientado al uso profesional o en entornos de trabajo con importantes recursos informáticos, en donde es necesario administrar una gran cantidad de equipos en cuanto a actualizaciones, creación de programas o archivos centralizados para poder acceder a los recursos de forma remota desde las estaciones de trabajo. [6]

Al ser una herramienta de administración de infraestructura, se hace un objetivo fundamental de ataque para los ciberdelincuentes, debido al riesgo que conlleva para la compañía si se vulnera dicha administración. Técnicas como "Kerberoast", el cual contiene un conjunto de herramientas para realizar un ataque a este servicio, "Pass The Hash" para realizar movimientos laterales en las máquinas que se encuentran en el mismo entorno, incluso técnicas como "GoldenTicket", las cuales se aprovechan del acceso que configuran los administradores cuando deben manejar una gran cantidad de accesos o cuentas del Sistema, o malas configuraciones por parte del equipo de TI al momento de iniciar el directorio activo, exceso de privilegios para los grupos o usuarios que realizan tareas sobre el Sistema. [6]

Los administradores de esta infraestructura son los más atacados mediante campañas de Phishing o Ingeniería Social, por los privilegios que cuentan sobre el Sistema, por ejemplo, con una configuración específica en el directorio es posible eliminar la fecha de caducidad de las contraseñas de los usuarios; es decir, si un ciberdelincuente logra acceder a estas credenciales

y el ataque no es alertado/detenido, lo más probable es que permanezcan el tiempo suficiente para preparar un ataque a gran escala contra la compañía dentro del Sistema sin ser descubiertos. [6]

VII. Arquitectura

En la figura 2 podemos ver la arquitectura que se implementó en la parte práctica de esta investigación. Y la función de cada uno de los componentes en esta arquitectura es:

- **Host 1:** es un Servidor local.
- **Host 2:** es un Servidor remoto.
- **Conjur:** asegura el acceso controlando estrictamente los secretos con el control de acceso basado en roles (RBAC) granular. Autentica la solicitud de acceso de una aplicación a un recurso, por medio de una verificación de autorización contra la política de seguridad y luego distribuye de forma segura el secreto. **[?]**
- **Ansible:** es una plataforma de Software libre para configurar y administrar ordenadores, considerada una herramienta de orquestación.

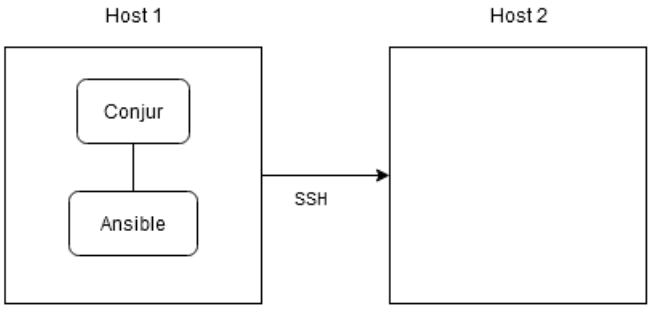

Fig. 2. Arquitectura implementada

Se cuenta con dos servidores, uno principal local (administrador) y uno secundario remoto, con sus respectivos usuarios y direcciones IP.

VIII. Resultados

La parte práctica consistió en crear un Playbook con su dirección IP, usuario y contraseña, luego crear el Ansible para el Playbook. Logrando identificar así, que si un ciberdelincuente logró acceder al Sistema, a través del Playbook va a poder ver toda la información en texto plano, por ende, se puso a prueba el funcionamiento de Conjur ofrecido por CyberArk como solución PAM, para evitar así que personas inescrupulosas que logren acceder al Sistema vean fácilmente esta información.

Para ello, Conjur inicializa un ambiente de trabajo con la ayuda de un Contenedor, posteriormente se crea una cuenta para la demostración y se inicializa Conjur CLI (si nos devuelve un mensaje de error es porque el sistema se está iniciando, se debe esperar un momento y volver a intentar), después de generarse el token, se inicia sesión en Conjur (como demostración se guardó el api_key en el archivo admin.out y como variable de entorno api_key, pero esta api_key se debe mantener en un lugar totalmente seguro).

Las políticas de muestra las ofreció Conjur, al revisar se obtuvieron políticas para root de Conjur, del Servidor y de Ansible. Se copiaron estos 3 archivos en el Contenedor del CLI de Conjur. Seguidamente, se asigna un ID de aplicación al Servidor de Ansible, se obtuvo el certificado SSL de Conjur CLI y se creó un token de fábrica de host, el cual se guardó como variable de entorno. Después, se preparó un archivo de inventario y un Playbook para concederle al anfitrión Ansible la identidad de Conjur.

Para finalizar, se centralizaron los Secretos (la información que se desea proteger) para agregarlos a Conjur. ¿Qué se va a proteger? Las direcciones IPs, los usuarios y las contraseñas de los Servidores. Se convirtió la identidad de Conjur para que fuera compatible con Ansible, se revisó el inventario de muestra que almacena los 2 servidores, se ejecutó el Playbook y se revisó nuevamente el archivo de inventario para determinar si se podía encontrar algún secreto incrustado en caso de que algún ciberdelincuente accediera al Sistema.

IX. Conclusiones

Al realizar la parte práctica se obtuvo que así logren ingresar los ciberdelincuentes al Sistema, la información estará protegida y lo único que verá es que se manejan dos ambientes, el host 1 y el host 2.

La instalación de las herramientas PAM es explícita, cuenta con gran documentación la mayoría de estas, a excepción de algunas pocas. En este ámbito existen diversas herramientas para ciertas especificaciones, por ejemplo Bastillion, Web Terminal o Pritunl Zero, son herramientas que nos facilitan una administración del entorno, ya sea para servicios, usuarios, servidores, entre otros; también, podemos contemplar herramientas como Conjur, que además de gestionar usuarios y entornos, nos facilita la protección de la información; con ayuda de su configuración es posible proteger la información sensible que está visible para los usuarios del sistema, evitando que estos observen más de la cuenta y asegurándonos que solo sea posible observar lo necesario.

Tener un control sobre el sistema es vital para contener fugas o uso indebido de los usuarios y acciones sobre el entorno, de esta manera se facilita la detección de usuarios no autorizados, por consiguiente, si se realiza una temprana detección, es posible evitar un impacto crítico a la organización.

REFERENCES

[1] CoreSecurity, "Gestión de acceso privilegiado." https://www.coresecurity.com/privileged-access-management. Accessed on 2021-09-20.

[2] OSIRIUM, "Introducción a la gestión de acceso privilegiado." https://www.osirium.com/resources/privileged-access-management. Accessed on 2021-09-20.

[3] IBM, "Permisos de acceso simples y granulares." https://www.ibm.com/docs/es/cognos-analytics/11.0.0?topic=permissions-simple-granular-access. Accessed on 2021-11-25.

[4] ISC, "¿qué es el cuadrante mágico de gartner y para qué sirve en transformación digital?." https://www.isc.cl/que-es-el-cuadrante-magico-de-gartner-transformacion-digital/. Accessed on 2021-10-04.

[5] Gartner, "Magic quadrant for privileged access management." https://www.gartner.com/doc/reprints?id=1-26UL30OG&ct=210719&st=sb&previtm=661624844&prevcol=7290074&ts=319681. Accessed on 2021-10-04.

[6] J. A. Castillo, "Active directory, qué es y para qué sirveb." https://www.profesionalreview.com/2018/12/15/active-directory/. Accessed on 2021-10-05.