Implementación de un Sistema de Autenticación y Gestión de Acceso PAM.

PROYECTO DE TITULACIÓN.

Autor: Andrés David Loor Villamar
Guía: Roque Jacinto Hernández Bustos

Presentado como parte de los requisitos para el Título de Magíster en Ciberseguridad.
CES: RPC-SE-01-N°.014-2020. Cohort2 2022 - 2023.
Correo electrónico del autor: andres.loor@casagrande.edu.ec
Guayaquil, **1 de marzo de 2023**.

Introducción

En la actualidad, la seguridad informática y la ciberseguridad son temas de gran importancia en las empresas y organizaciones que manejan información confidencial, razón por la cual deben estar preparados para proteger sus sistemas y datos de posibles amenazas y ataques cibernéticos. Para lograr una gestión de la seguridad eficiente, la implementación de un PAM por sus siglas en inglés (Privileged Access Management) se convierte en una herramienta esencial para controlar el acceso y privilegios de las cuentas administradores y/o cuentas con privilegios elevados a los recursos críticos para la organización. La implementación de un PAM permite a las empresas reducir el riesgo de fraude, proteger la información confidencial y cumplir con regulaciones de entidades de control. En mi proyecto de titulación de la Maestría en Ciberseguridad escogí seis materias que fueron de gran importancia para el impulso de la propuesta y posterior implementación en mi lugar de trabajo donde se analiza la importancia y beneficios de un Sistema de Autenticación y Gestión de Accesos PAM.

Resumen

El presente trabajo de titulación tiene como objetivo principal la implementación de un sistema de gestión de accesos privilegiados (PAM por sus siglas en inglés) en una organización. Para ello, se realizó una evaluación inicial en la cual se identificaron riesgos asociados al uso de las cuentas categorizadas como críticas con privilegios de accesos a los servicios y componentes críticos en su sistema.

A partir de esta evaluación, se sugirió y se impulsó la implementación de una solución PAM que se ajusta a las necesidades y características de la organización y se procedió a su implementación. Se realizaron pruebas y verificación para garantizar el correcto funcionamiento del sistema y se actualizaron las políticas actuales de accesos en función al tipo de acceso y flujo de aprobación para el uso de las cuentas privilegiadas en la empresa, salvaguardando la triada de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Los resultados obtenidos indican que la implementación del PAM fortalecerá la seguridad de la información en la organización, al permitir un mayor control y monitoreo de las cuentas con privilegios elevados de acceso.

Objetivo

El objetivo de este ensayo integrador es describir la importancia de la implementación de un Sistema de Autenticación y Gestión de Acceso PAM en las organizaciones y los beneficios que puede aportar en términos de seguridad informática y ciberseguridad. Adicionalmente, este ensayo enlaza la implementación de este proyecto con las habilidades y conocimientos adquiridos durante el programa de Maestría en Ciberseguridad.

Desarrollo

Gerencia, Operaciones y Planificación de la Ciberseguridad.

En esta materia se impartieron los conocimientos necesarios para comprender y dar relevancia del control interno, donde se resalta que "El control interno ayuda a las entidades a lograr importantes objetivos y a mantener y mejorar su rendimiento" (Carranza Benalcázar, A. R., 2017). Dentro de las clases magistrales cambió la perspectiva alineando los objetivos institucionales a los objetivos de IT y controles respectivos, donde cada empresa tiene un contexto diferente y este contexto está determinado por factores externos e internos y requiere de un sistema de gobierno y gestión personalizado (Hernández Hernández, J, 2018).

Se destacó también la norma ISO 27001 – 27002:2013 el cual son dos estándares complementarios que abordan el Sistema de Gestión de la Seguridad de la Información (SGSI) y proporciona un marco para la evaluación y tratamiento de los riesgos de seguridad. La norma ISO 27002 proporciona las directrices para la implementación de controles de seguridad de la información. En conjunto, estas normas ayudan a las organizaciones a proteger sus activos de información y mitigar los riesgos de seguridad de manera más efectiva (Lino López, J. J. 2021).

Tecnología, Modelos y Técnicas de Ciberseguridad.

Esta asignatura se centró en una introducción completa de la ciberseguridad, incluyendo la historia de la ciberseguridad, las amenazas y vulnerabilidades comunes. Así también los principios de la criptografía, los controles de seguridad, la gestión de riesgos, gestores de contraseña y la seguridad de la red. Además, se aprendió todas las dimensiones de la ciberseguridad: confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad (ISACA, 2017).

Estrategias y Políticas Multilaterales para la Ciberseguridad.

La materia contempló una visión general de la seguridad integral y la importancia de la estrategia de la seguridad de la información mediante el Esquema Gubernamental del EGSI (Muyón, C., Guarda, T., Vargas, G., & Quiña, G. N. 2019). Que mediante este esquema pretende preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión del riesgo de seguridad de la información y así también la selección de los controles para el tratamiento de los riesgos identificados.

Hacking Ético y Análisis del Ciberataque.

El hacking ético es una práctica que busca mejorar la seguridad informática y ciberseguridad, donde se destacaron el uso de técnicas y herramientas similares a las que utilizan los hackers malintencionados o ciberdelincuentes, pero con el objetivo de identificar y corregir vulnerabilidades en los sistemas de información de una organización (Pacheco, F. G., & Jara, H. 2010). Indicó también las definiciones y conceptos de la seguridad informática, sobre la tríada CIA (Confidencialidad, Integridad y Disponibilidad) y otros conceptos como autorización, autenticación e identificación.

Continuidad del Negocio.

En esta materia aprendimos la importancia de la continuidad del negocio no solo desde un punto de vista de tecnología y seguridad si no de empresa contemplando los procesos más críticos para el negocio, por medio de medidas preventivas y acciones necesarias para mantener las operaciones mínimas aceptables durante una contingencia. (Martínez, J. G., 2010)

Implementación

Un Sistema de Autenticación y Gestión de Acceso PAM.

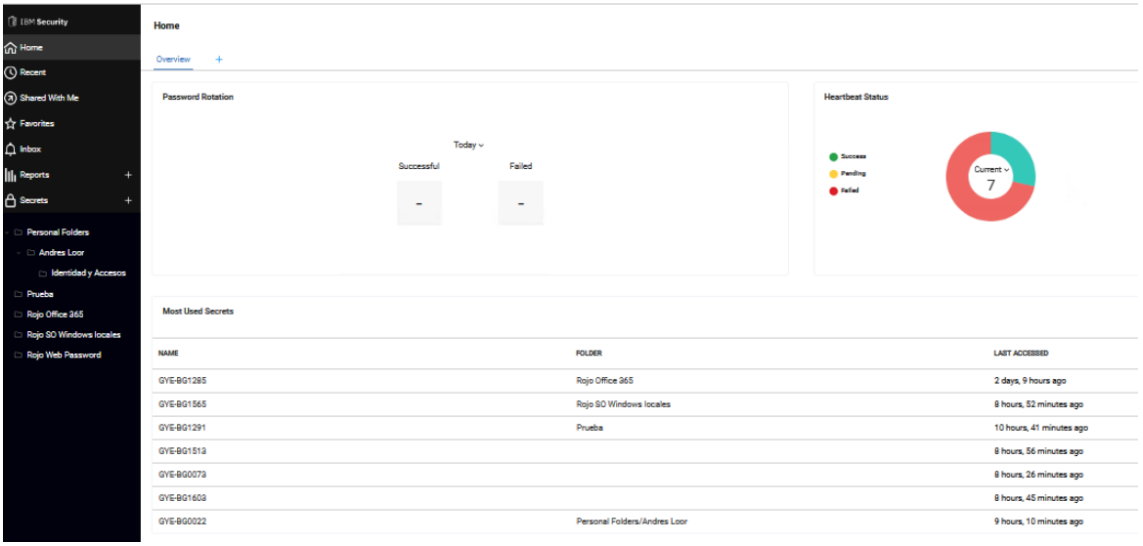
Las empresas, independientemente de su giro de negocio, ya sean del ámbito tecnológico o no, manejan una cantidad importante de servicios y procesos, cada uno de estos servicios o procesos tiene asociado diferentes usuarios y sus correspondientes credenciales (usuario y contraseña) con diferentes niveles de permisos y roles asociados, por lo tanto surge la necesidad de herramienta que faciliten, tanto a los administradores de los sistemas, usuarios de los mismos el uso de manera correcta de sus credenciales y administradores de seguridad la tarea de mantenimiento y revisión de dichas autenticaciones. En el presente proyecto de Implementación del Sistema de Autenticación y Gestión de Acceso PAM, se describen los beneficios para controlar el acceso a cuentas con privilegios elevados, actualización de políticas de uso de cuentas privilegiadas y contraseñas.

Para la implementación del gestor de contraseña en la empresa donde laboro se impulsó la herramienta de IBM Secret Server- Security Verify Privilege Vault el cual es suficientemente flexible y abarca un amplio espectro de integración con tipos de accesos o subsistemas que se incorporan bien a los diferentes componentes y servicios críticos de la institución que tienen autenticación con cuentas de máximos privilegios.

Tal como se observa en la Figura 1, el front de la página de bóveda virtual IBM Secret Server- Security Verify Privilege Vault.

Figura 1

El home de la implementación del Sistema de autenticación y Gestor de accesos PAM



Nota. Auditoría propia de la implementación.

Dentro de las características principales del PAM de IBM Secret Server- Security Verify Privilege Vault, es el descubrimiento de cuentas desconocidas mediante un agente instalado en los endpoint que identifica dispositivos, servidores y otros puntos finales con privilegios administrativos para hacer cumplir la seguridad con privilegios mínimos, controlar los derechos de las aplicaciones y reducir el impacto en los equipos de soporte.

También tenemos el restablecimiento de contraseñas de forma automática ajustándose a la política de contraseña como puede ser la complejidad, longitud etc. Supervisa, monitorea y realiza grabaciones de las actividades que se realizan con las cuentas privilegiadas facilitando el control interno ya sea por auditoría o control de acceso a lo largo del ciclo de vida de la cuenta privilegiada.

Principales ventajas.

Una de sus principales características es:

- La mitigación de amenazas de seguridad modernas de explotación de aplicaciones mediante la eliminación de los derechos administrativos locales de servidores y dispositivos.
- Detecta e integra automáticamente credenciales y secretos con privilegios utilizados por entidades humanas y no humanas.
- La administración centralizada de políticas permite a los administradores establecer las mismas, para la complejidad de las contraseñas, su frecuencia de rotación, qué usuarios pueden acceder a qué cajas fuertes y mucho más.
- La rotación automatizada de contraseñas ayuda a reforzar la seguridad a la vez que elimina los procesos manuales que requieren mucho tiempo para los equipos de TI.

Dentro del proceso de implementación del Sistema de Autenticación y Gestión de accesos PAM con Security Verify Privilege Vault de IBM, se detalla lo siguiente

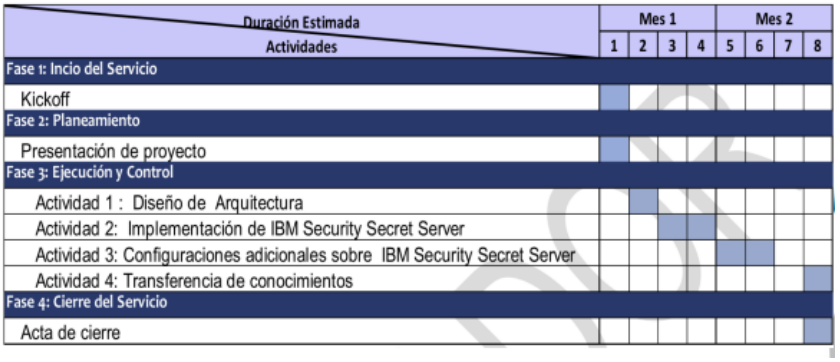
Fase de implementación.

En función al cronograma establecido se detallan las tareas macros que se definieron para la implementación del Sistema de Autenticación y Gestión de Accesos PAM, las cuales se contemplaron en el kickoff del proyecto, así también la revisión de prerrequisitos entregados para la implementación, definición de la matriz de roles y responsabilidades entre el proveedor y el equipo que llevamos adelante el proyecto.

Tal como se observa en la Figura 2, el detalle de las actividades macro del proyecto.

Figura 2

Cronograma del proyecto.



Duración Estimada / Actividades	Mes 1				Mes 2			
	1	2	3	4	5	6	7	8
Fase 1: Incio del Servicio								
Kickoff								
Fase 2: Planeamiento								
Presentación de proyecto								
Fase 3: Ejecución y Control								
Actividad 1 : Diseño de Arquitectura								
Actividad 2: Implementación de IBM Security Secret Server								
Actividad 3: Configuraciones adicionales sobre IBM Security Secret Server								
Actividad 4: Transferencia de conocimientos								
Fase 4: Cierre del Servicio								
Acta de cierre								

Nota. Auditoría propia de la implementación.

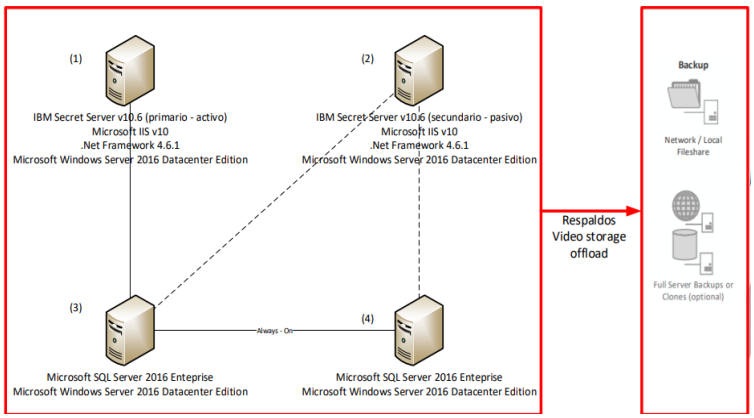
Arquitectura de la solución y prerrequisitos.

Se definió una arquitectura con 2 servidores de servicios activo - pasivo para garantizar redundancia y alta disponibilidad en el servicio de la bóveda virtual con 2 servidores Always On y con plan de respaldos de acuerdo a la política por ser un componente crítico.

Tal como se observa en la Figura 3, la arquitectura de la implementación con alta disponibilidad.

Figura 3

Arquitectura de la Implementación del Sistema de autenticación y Gestor de accesos PAM.



Nota. Auditoría propia de la implementación.

Según como se observa en la Figura 4, se detallan los requisitos con los que se solicitó la instalación de la solución del proyecto de bóveda virtual Sistema de autenticación y Gestión de Accesos PAM.

Figura 4

Requisitos de los servidores para la implementación.

Node	Hardware (total)	Máquina Virtual (VM)	Software
(1) Secret Server – Activo	CPU: 4 vCores RAM: 16GB Disco: 200 GB	VMWare ESX Server v6.x o posterior	IBM Secret Server v11 Microsoft IIS v10 .Net Framework 4.8 o posterior Microsoft Windows Server 2019
(2) Secret Server - Pasivo	CPU: 4 vCores RAM: 16GB Disco: 200 GB		IBM Secret Server v11 Microsoft IIS v10 .Net Framework 4.8 Microsoft Windows Server 2019
(3) Base de Batos - Primario	CPU: 8 vCores RAM: 32 GB Disco: 1.5 TB		Microsoft Windows Server 2019 – Enterprise Collation SQL_Latin1_General_CP1_CI_AS

Nota. Auditoría propia de la implementación.

Situación actual de la institución financiera.

La situación actual, del proceso de gestión de cuentas privilegiadas es que se llevaba registros manuales tanto para el inventario de cuentas privilegiadas como registros en bitácoras de los sobres físicos como de las credenciales enviadas por correo electrónico para tener trazabilidad del uso y actualización de cambio de contraseñas con controles RMS, por la cual el proceso actual podría estar expuesto a una serie de riesgos de seguridad.

- Vulnerabilidades de autenticación.
- Accesos no autorizados.
- Cumplimiento a medias de regulaciones normativas.

Estrategia de implementación.

Al ser un proceso crítico que soporta todas las cuentas que apalancan los servicios tecnológicos o humanos con privilegios elevados para el negocio se tomó en consideración varias aristas que ayudaron a validar en función al tipo de acceso de la cuenta o como se la denomina en la solución de bóveda virtual y gestión de accesos PAM (secretos).

A continuación, se detalla el cronograma de configuración y validación en función a los tipos de secretos.

Según como se observa en la Figura 5, se detalla el plan maestro para la implementación.

Figura 5

Plan maestro de la implementación.

Id	Task Name	% completado	Duración
1	**PRY_IBM Secuity Secret Server - Banco Guayaquil**	**49%**	**63.4 días**
2	**Fase 1: Inicio de Proyecto y Fase 2 : Planificación**	100%	1 día
3	**Fase 2: Planificación**	100%	4 días
4	**Fase 3: Ejecución y Control**	**46%**	**51.4 días**
5	Preparación de ambiente	100%	20 días
6	Configuración balanceador	0%	1 día
7	**Actividad 1 : Diseño de Arquitectura**	**29%**	**18.5 días**
8	Análisis de la Arquitectura física de la solución	100%	1 día
9	Presentación de recomendaciones/findings y la Arquitectura recomendada	0%	0.5 días
10	Documentación conceptual de arquitectura	0%	2 días
11	**Actividad 2: Implementación de IBM Security Verify Privilege Vault**	**35%**	**13.5 días**
12	Validación de pre-requisitos de hardware y software y preparación del ambiente.	100%	1 día
13	Configuración de SQL Server en HA	100%	0.5 días
14	Configuración de IIS en HA	50%	2 días
15	Instalación de .NET Framework	100%	0.5 días
16	Implementación de IBM Security Verify Privilege Vault en HA (2 nodos como ACTIVO-ACTIVO)	50%	5 días
17	Configuración de autenticación integrada a Active Directory	0%	0.5 días
18	Creación de hasta 10 usuarios. Configuración de grupos y roles default	0%	0.5 días
19	Configuración de estructuras de carpetas	0%	0.5 días
20	Creación de hasta 20 secretos basados en templates default, configuración de políticas y su expiración	0%	5 días
21	**Actividad 3: Configuraciones adicionales sobre IBM Security Verify Privilege Vault**	**0%**	**13.9 días**

Id	Task Name	% completado	Duración
22	Integración de cinco (5) fuentes Microsoft Windows MSRPC	0%	6 días
23	Configuración Session recording para MS Windows RDP y Putty/SSH default launchers.	0%	0.5 días
24	Configuración de funcionalidad de checkout para hasta cinco (5) secretos	0%	0.5 días
25	Configuración de cambio de contraseña en check in usando default password changers	0%	0.5 días
26	Configuración de workflow simple para access request para hasta cinco (5) secretos	0%	1 día
27	Configuración de Remote Password Change (RPC) para hasta cinco (5) cuentas de servicio	0%	1 día
28	Habilitación de syslog para integración con SIEM	0%	0.2 días
29	Validación de auditoria sobre reportes default	0%	0.2 días
30	Pruebas funcionales	0%	1 día
31	Documentación de la implementación, operación y procedimientos de backup & restore	0%	3 días
32	**Actividad 4: Transferencia de conocimientos**	**0%**	**4 días**
33	Preparación de transferencia de conocimientos Security Verify Privilege Vault	0%	2 días
34	Transferencia de conocimientos Security Verify Privilege Vault (2 sesiones de 4 horas)	0%	2 días
35	**Fase 4: Cierre**	0%	2 días

Nota. Auditoría propia de la implementación.

Estrategias de pruebas.

Coordinación con cada una de las áreas de IT las validaciones de los flujos de aprobación, políticas de los secretos, tipos de accesos y revisión/validación de las pruebas mediante check list que garanticen el no comprometer las credenciales. Para esto se realizó en la fase inicial del proyecto entregables en función a diversos escenarios de acuerdo al tipo de acceso con las diferentes casuísticas de las cuentas inventariadas y posterior masificación en fases controladas, en la que nos encontramos actualmente.

Entregable fase inicial.

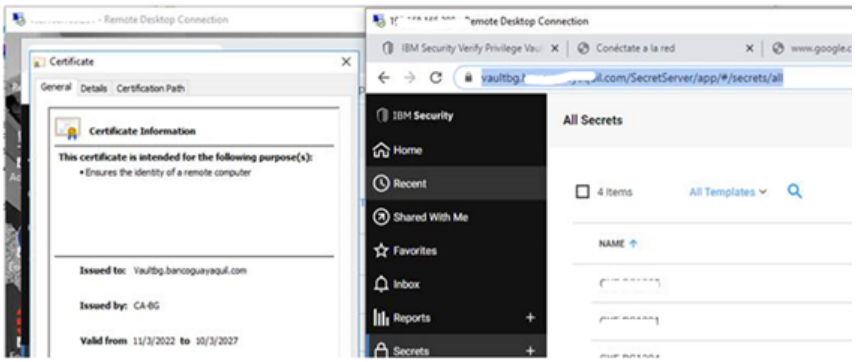
A continuación se detallan los entregables de la fase inicial realizados durante la implementación del proyecto.

- **Criptografía y permisos de comunicación.**

Tal como se observa en la Figura 6, los permisos de comunicación sólo desde los servidores bastiones y con instalación de certificado digital de la página con https a nivel de balanceador y complementos instalados a nivel navegador para el Sistema de Autenticación y Gestión de Accesos PAM con Security Verify Privilege Vault de IBM.

Figura 6

Página con certificado digital.



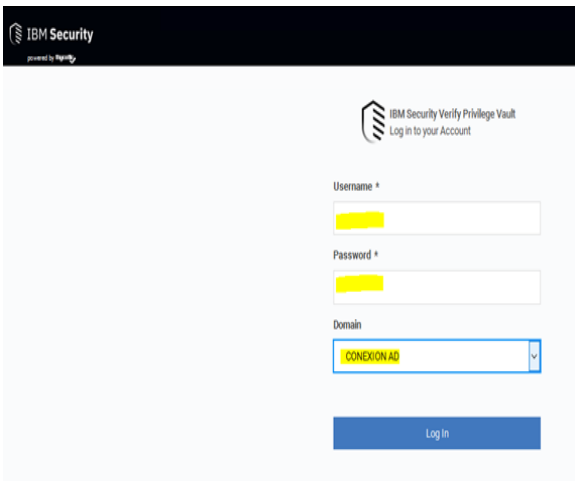
Nota. Auditoría propia de la implementación.

- **Integración de autenticación de la bóveda virtual con Directorio Activo.**

Según se observa en la Figura 7, se valida la integración con login de usuario de dominio autorizado.

Figura 7

Autenticación con Directorio Activo.



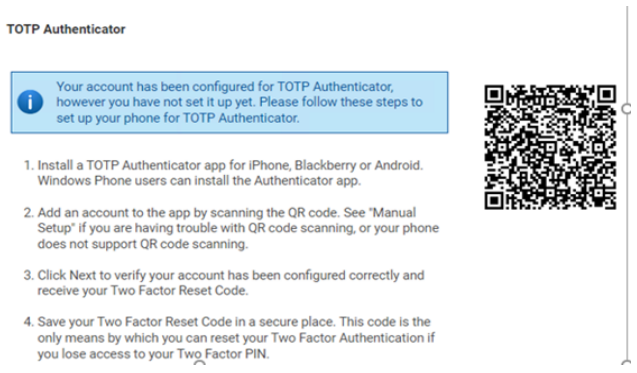
Nota. Auditoría propia de la implementación.

- **Habilitación de usuarios creados con doble factor de autenticación.**

De Acuerdo a lo observado en la Figura 8, se confirma la exigencia después del login del segundo factor de autenticación para los usuarios de la bóveda virtual.

Figura 8

Segundo factor de autenticación habilitado y exigido.



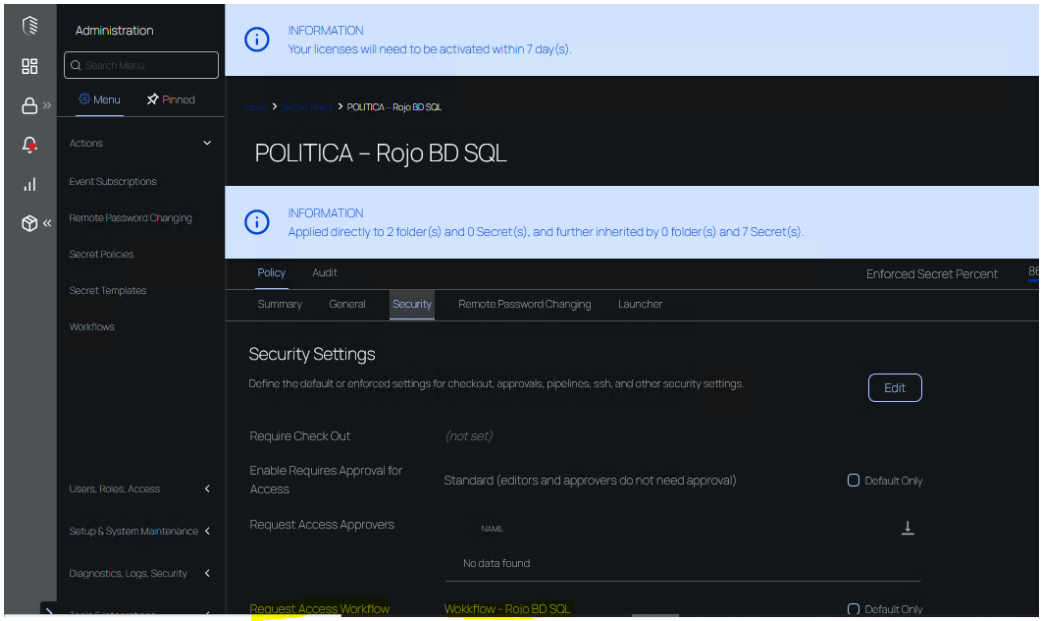
Nota. Auditoría propia de la implementación.

- **Creación de políticas.**

Como detallo en la Figura 9, la creación de la política de bóveda virtual la cual como base tiene implícitamente el flujo de aprobación, ejecución del lanzador, ejecución en modo incógnito para tipos de accesos web, cambio remoto de claves después de utilizar una cuenta entre otras configuraciones.

Figura 9

Política ejemplo para tipos de cuenta SQL Management.



Nota. Auditoría propia de la implementación.

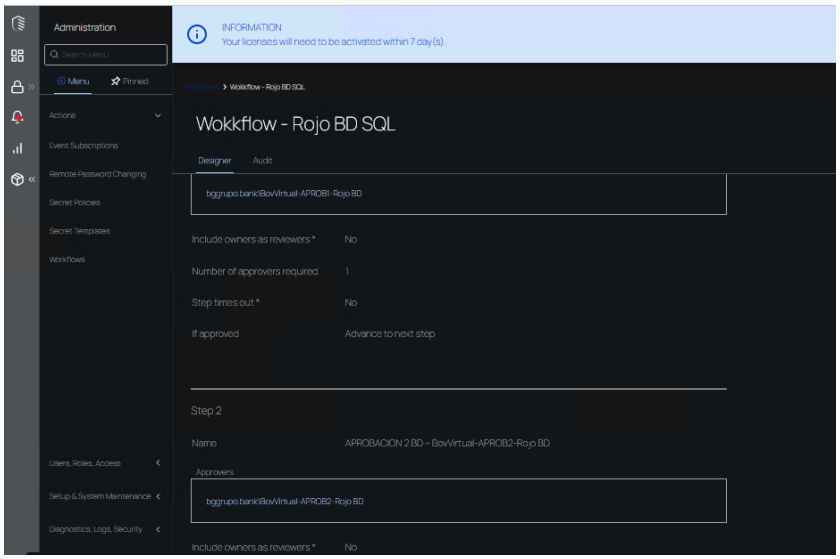
- **Asignación de permisos a nivel de carpeta para asociar secretos y flujos de aprobación.**

Tal como se observa en la Figura 10, los creación del flujo de aprobación para tipos de cuentas o secretos SQL Management el cual está establecido por el nivel jerárquico de los solicitantes autorizados. Ejemplo para un Oficial de Base de datos el flujo de aprobación es el siguiente:

- ☐ Aprobación 1 - Sub gerencia de Base de Datos.
- ☐ Aprobación 2 - Gerencia de Base de Datos.
- ☐ Aprobación 3 - Gerencia de Seguridad de la Información.

Figura 10

Flujo de aprobación para tipo de cuentas SQL Management.



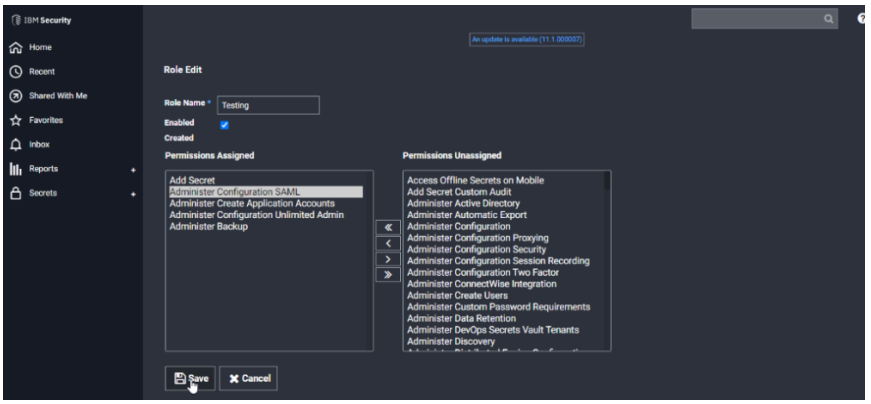
Nota. Auditoría propia de la implementación.

- **Creación de roles de acuerdo a grupos de AD y detalle de los permisos.**

Según se observa en la Figura 11, el detalle de la creación de roles personalizados con permisos granulares, solo para las áreas involucradas en la implementación.

Figura 11

Creación de roles para la bóveda virtual.



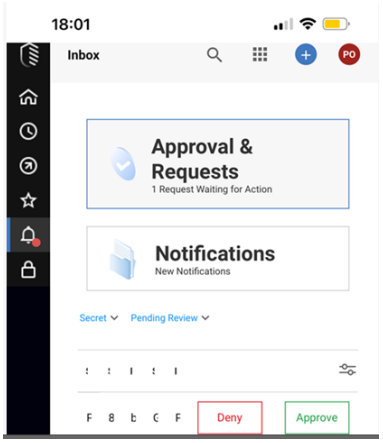
Nota. Auditoría propia de la implementación.

- **Pruebas controladas de flujo de solicitud y aprobación mediante la página de Bóveda Virtual, correo electrónico y móvil.**

Según se observa en la Figura 12, se evidencia la aprobación de las cuentas solicitadas por los solicitantes autorizados a través de dispositivo móvil, cabe indicar que también estás aprobaciones se pueden realizar por la url de la bóveda virtual.

Figura 12

Imagen de aprobación a través de dispositivos móviles.



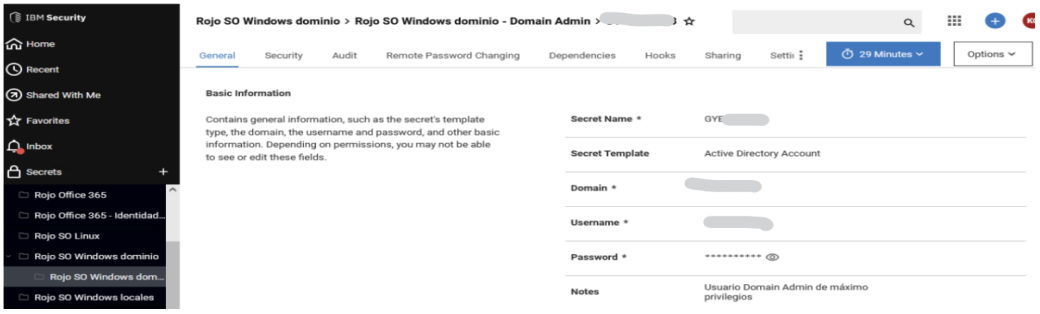
Nota. Auditoría propia de la implementación.

- **Prueba de lanzadores de secretos configurados – Web Server, Windows Account, Directorio Activo, Unix SSH y SQL Server**

Tal como se observa en las Figuras 13 al 16, se evidencia la prueba de lanzadores de acuerdo al tipo de secreto, para este ejemplo vía RDP (Escritorio remoto) desde la bóveda virtual.

Figura 13

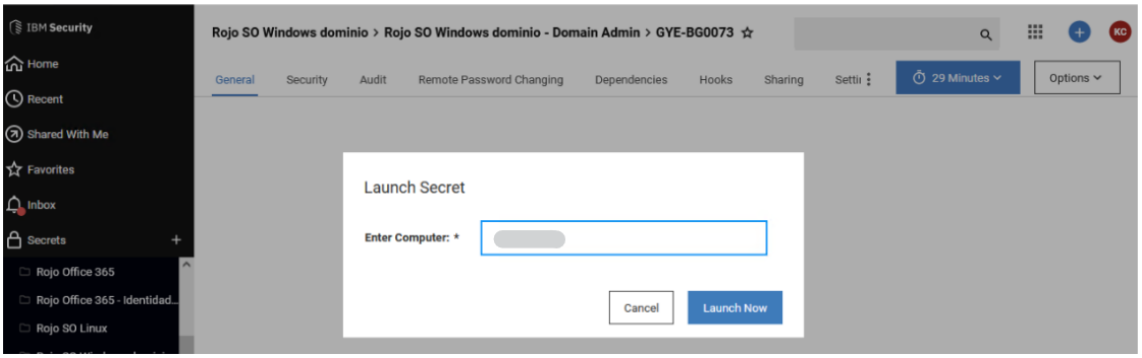
Configuración del secreto.



Nota. Auditoría propia de la implementación.

Figura 14

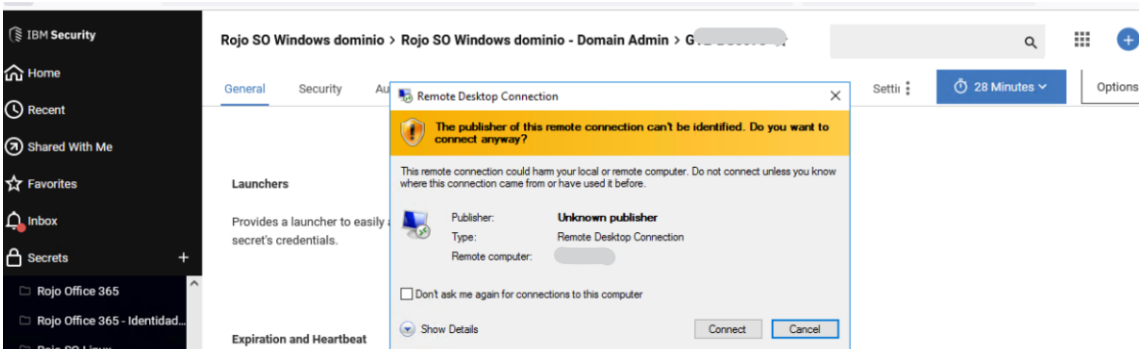
Ejecución del lanzador.



Nota. Auditoría propia de la implementación.

Figura 15

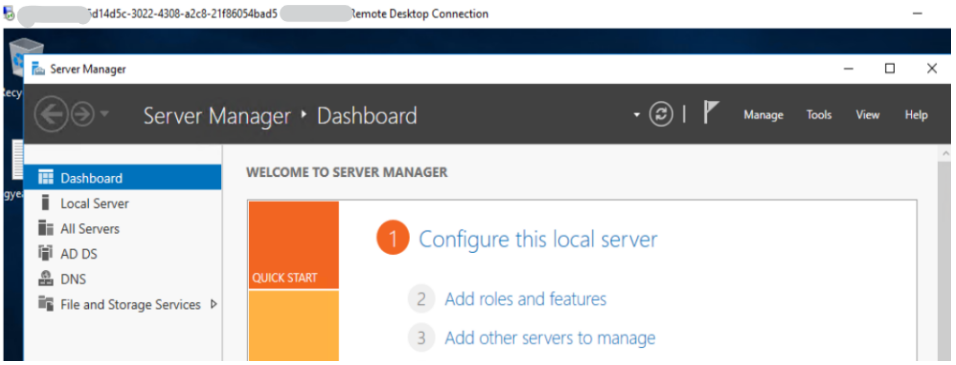
Evidencia de ejecución del lanzador sin comprometer credenciales.



Nota. Auditoría propia de la implementación.

Figura 16

Carga del inicio de sesión vía RDP con las credenciales del secreto.



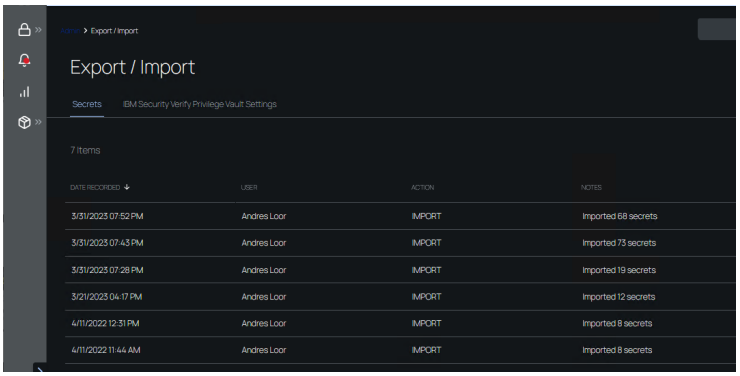
Nota. Auditoría propia de la implementación.

- **Subir masivamente secretos mediante archivos csv.**

  Como detallo en la Figura 17, la evidencia para subir secretos de forma masiva.

Figura 17

Evidencia de ejecución de importación de secretos por archivo csv.



Nota. Auditoría propia de la implementación.

- **Creación de notificaciones.**

Se evidencia en la Figura 18, notificaciones mediante check out / check in cuando un administrador edita o accede a las configuraciones de un secreto que debe comprometer la contraseña.

Figura 18

Evidencia de check out / check in.

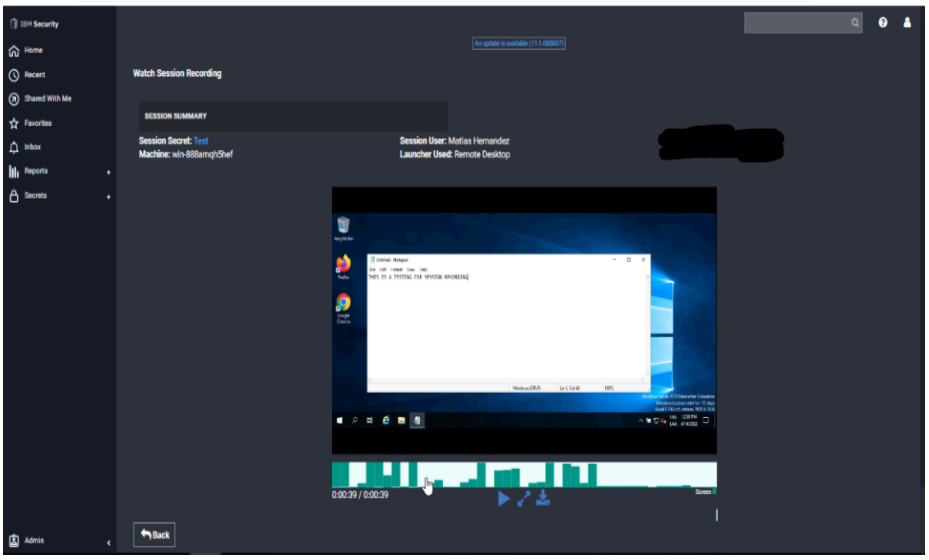
Nota. Auditoría propia de la implementación.

- **Grabación de sesiones.**

Tal como se evidencia en la Figura 19, se muestra la evidencia de grabación de las acciones ejecutadas con el usuario de privilegios elevados para tener visibilidad de las tareas que se ejecutó con el usuario.

Figura 19

Grabaciones de sesión de usuario con privilegios elevados que solicitó la cuenta.



Nota. Auditoría propia de la implementación.

- **Monitoreo.**

Tal como se evidencia en la Figura 20, se muestra la evidencia del dashboard para la gestión e indicadores a nivel de secreto en la bóveda virtual.

Figura 20

Dashboard de la implementación del sistema de Autenticación y Gestión de Accesos.

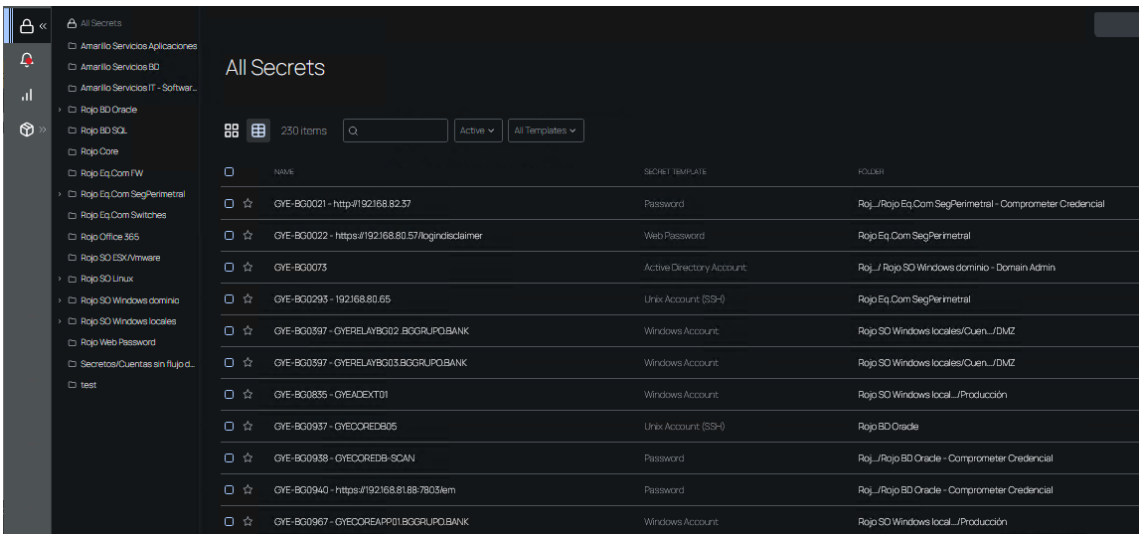
Nota. Auditoría propia de la implementación.

- **Estructura de secretos de la solución del Sistema de autenticación y Gestión de Accesos PAM.**

Evidenciamos en la Figura 21, la estructura final de la fase inicial del proyecto de implementación para posterior volcado de las demás cuentas.

Figura 21

Estructura actual de la implementación.



Nota. Auditoría propia de la implementación.

Esquema actual de operación nuevos secretos.

Se detalla el esquema actual para los requerimientos de creación de nuevos secretos.

- Ingreso del requerimiento a través del sistema de incidentes, el cual debe estar adjunto formulario de creación de secretos, donde detallan los datos requeridos obligatorios para configuración en la bóveda virtual de la cuenta.

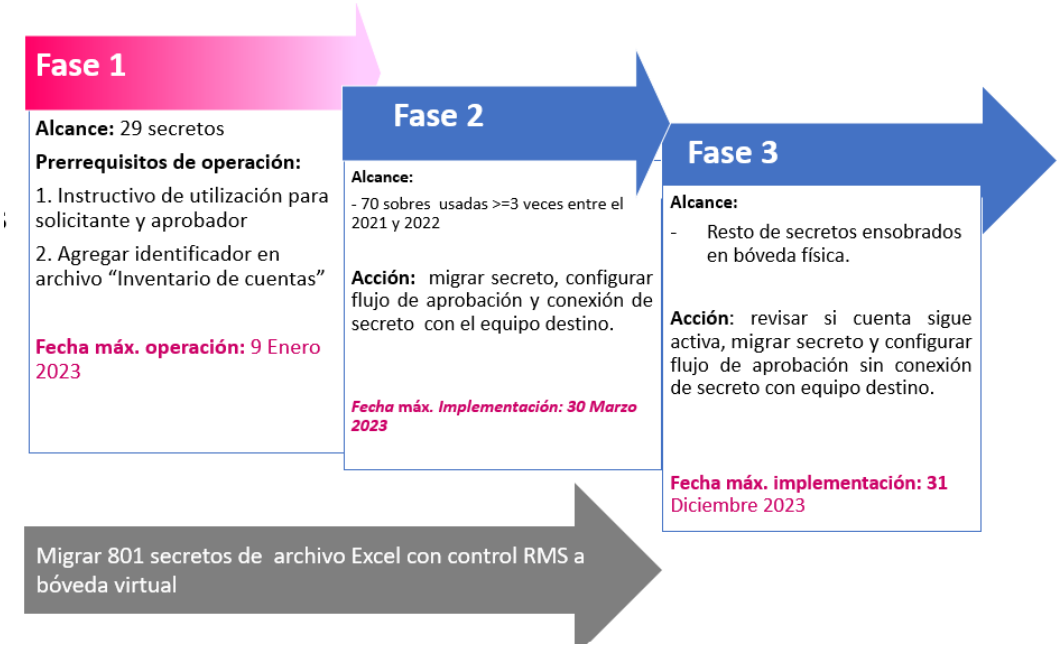
Fases de masificación actual.

Se detalla la estrategia para el volcado de todas las cuentas de privilegios elevados que actualmente se encuentran inventariadas que suman un total de más de 2000 cuentas o secretos..

Tal como se observa en la Figura 22, se detalla las siguientes fases para el volcado final de las cuentas que se tienen inventariadas de forma manual a la bóveda virtual Sistema de autenticación y Gestión de Accesos PAM.

Figura 22

Volcado de cuentas a la Bóveda Virtual.



Nota. Auditoría propia de la implementación.

Conclusiones

La implementación de un sistema de gestión de autenticación y gestión de accesos PAM es una tarea crítica para cualquier organización que quiera asegurar la seguridad de sus recursos y datos confidenciales. Dentro de una implementación exitosa tenemos las siguientes conclusiones:

Aumento de la seguridad. La implementación del sistema de gestión de autenticación y gestión de accesos PAM permitió restringir el acceso a los recursos de la organización y solamente a aquellos usuarios que realmente necesitan acceder a ellos. Además, permite monitorear y auditar el acceso a los recursos, lo que contribuye a la detección y prevención de posibles amenazas de seguridad.

Reducción del riesgo. Un sistema PAM reduce significativamente el riesgo de que un usuario malintencionado o no autorizado tenga acceso a los recursos críticos de la organización.

Mejora de la productividad. La implementación del sistema PAM mejoró la productividad de los empleados al eliminar la necesidad de recordar múltiples credenciales y permitir el acceso a los recursos de forma más rápida y sencilla.

Cumplimiento normativo. Un sistema PAM ayudó a la organización a cumplir con los requisitos normativos y regulatorios en cuanto a la protección de datos y la gestión de accesos, lo que puede ser un factor crítico para evitar sanciones o multas.

Recomendaciones

Capacitación a los usuarios. La capacitación de los usuarios es una parte importante, dado que deben estar informados de la política de seguridad y cómo utilizar la autenticación a través del Sistema de Gestión de accesos PAM.

Realizar pruebas de penetración. Las pruebas de penetración pueden ayudar a detectar vulnerabilidades en el sistema de autenticación y cómo los atacantes pueden intentar explotarlas. Es importante realizar pruebas regulares y actualizar las políticas de seguridad y configuraciones según los resultados.

Mantener actualizado el sistema. Es importante mantener actualizado el sistema de autenticación y gestión de accesos PAM. Las actualizaciones pueden incluir correcciones de seguridad y nuevas características que mejoren la seguridad del sistema. Es importante estar al tanto de las actualizaciones disponibles y aplicarlas según corresponda.

Realizar copias de seguridad regulares. Las copias de seguridad pueden ayudar a proteger la información crítica en caso de una falla del sistema o una violación de seguridad. Es importante realizar copias de seguridad regulares de la configuración del sistema y los registros de acceso y almacenarlas en un lugar seguro.

Limitaciones.

Dentro de las limitaciones encontradas para la implantación del Sistema de Autenticación y Gestión de Accesos PAM tenemos las siguientes:

Dependencia de la precisión de la información. Inventario de cuentas privilegiadas actual no se tiene identificado el tipo de acceso de la cuenta y se encuentra desactualizado.

Falta de adaptabilidad. Se puede tener dificultades para adaptar cambios a las políticas actuales como contraseñas y cuentas privilegiadas.

Costo y complejidad de implementación de un Sistema de Gestión de Accesos. La implementación puede ser muy costosa y compleja, especialmente para instituciones con sistemas y aplicaciones que necesitan ser integrados.

Referencias

Carranza Benalcázar, A. R. (2017). Estructura de control interno para la empresa Inyecplast CIA. LTDA. En base al modelo Coso 2013 (Bachelor's thesis, PUCE).

Hernández Hernández, J. (2018). COBIT, una metodología que genera valor en las empresas.

ISACA. (2017). Cybersecurity Fundamentals Study Guide (2nd ed.)

Lino López, J. J. (2021). Herramientas para mejorar la seguridad informática en ambientes de cómputo en el sector educación: una revisión de la literatura científica.

Martínez, J. G. (2010). El plan de continuidad de negocio: Una guia práctica para su elaboración. Ediciones Díaz de Santos.

Muyón, C., Guarda, T., Vargas, G., & Quiña, G. N. (2019). Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador. Revista Ibérica de Sistemas e Tecnologias de Información, (E18), 310-317.

Pacheco, F. G., & Jara, H. (2010). Hackers al descubierto. USERSHOP.

Glosario de Términos

Autorización. Proceso mediante el cual se determina a qué recurso puede acceder un usuario después de haber sido autenticado.

Autenticación multifactor. Método de autenticación que requiere más de un factor para verificar la identidad del usuario.

Sesión. Periodo de tiempo durante el cual un usuario tiene acceso a un recurso.

Privilegio. Permiso para acceder a un recurso o realizar una acción específica.

Gestión de accesos. Conjunto de procesos y tecnologías que controlan el acceso a los recursos de una organización.

Política de contraseñas. Conjunto de reglas que definen cómo deben ser las contraseñas de los usuarios y cómo deben ser gestionadas.

Contraseña. Secuencia de caracteres utilizada para autenticar la identidad de un usuario.

Gestión de contraseñas / Bóveda Virtual. Proceso de creación, almacenamiento y gestión de contraseñas de usuario.

Protocolo de autenticación. Conjunto de reglas que se utilizan para verificar la identidad de un usuario.

Protocolo de autorización. Conjunto de reglas que se utilizan para determinar a qué recursos puede acceder un usuario después de haber sido autenticado.

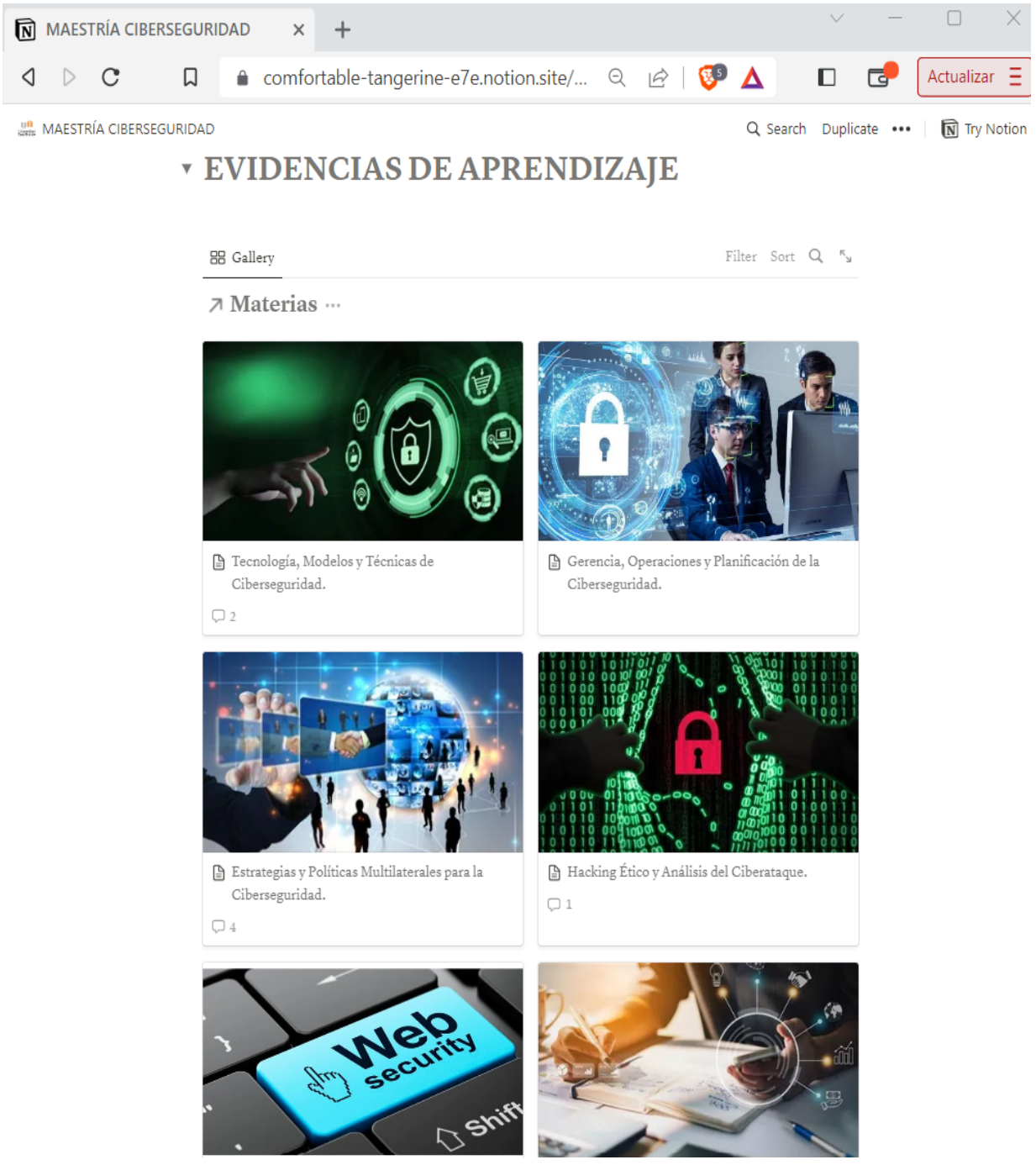
Token de autenticación. Cadena de caracteres que se utiliza para identificar y autenticar a un usuario.

Certificado digital. Archivo electrónico que contiene información sobre la identidad del titular y que se utiliza para verificar su autenticidad.

ANEXO 1

Evidencia de aprendizaje.

https://comfortable-tangerine-e7e.notion.site/MAESTR-A-CIBERSEGURIDAD-85284a3cb6754fb09ea9dc9f48069968



ANEXO 2

Propuesta de implementación.

https://prezi.com/view/kuvxJH1h97XSqKXiCgYy/