

## **Actividad 1. Diseminación del Conocimiento Organizacional**

**Ingeniería de Conocimiento**

**Ingeniería en Desarrollo de Software**

**Tutor: Aarón Iván Salazar Macías**

**Alumno: José Luis Pacheco González**

**Fecha: 12 de noviembre de 2024**

## Índice

Introducción .....	3
Descripción .....	4
Justificación .....	5
Desarrollo .....	6
• Reunión .....	6
• Escenarios de colaboración .....	8
• Diseño de la base de conocimiento y Procesos de adquisición de conocimiento .....	10
Conclusión .....	17
Referencias .....	18

## Introducción

La presente actividad aborda el diseño y desarrollo de una base de conocimiento segura, cuyo objetivo es salvaguardar y optimizar el acceso a la información crítica de la organización. Dada la importancia de la seguridad en el sector financiero, la propuesta se enfoca en la implementación de prácticas que protejan la confidencialidad, integridad y disponibilidad de los datos, adoptando una estructura de control de acceso y autenticación robusta, alineada con estándares actuales.

Para lograr un diseño que responda a estas necesidades, se detalla el uso de la plataforma Gather, la cual facilita la colaboración y el intercambio de ideas en un entorno virtual. La actividad incluye el diseño visual de la base de conocimiento, mostrando los niveles de acceso y controles de seguridad, junto con la documentación de procesos de adquisición de conocimiento interno y externo, tanto explícito como tácito. Este diseño permitirá a la institución mejorar su eficiencia y toma de decisiones, protegiendo al mismo tiempo la información sensible mediante un enfoque de “mínimos privilegios” y autenticación avanzada. La actividad concluye con la documentación del esquema de seguridad propuesto, integrando los puntos clave discutidos en equipo y organizando una estructura de fácil acceso y comprensión para todos los usuarios.

## Descripción

Este proyecto se centra en la creación de una base de conocimiento para una institución financiera, liderada por el nuevo Knowledge Management Officer (KMO). La base de conocimiento, concebida como un recurso clave para el área, busca organizar y proteger información crítica mediante un diseño que prioriza la seguridad. La propuesta incluye la estructuración del sistema de acceso y la implementación de procesos de adquisición de conocimiento que faciliten la recopilación y gestión de información tanto interna como externa.

Dado que la seguridad de la información es el mayor desafío, el proyecto requiere un diseño que restrinja y controle el acceso, asegurando que cada usuario pueda acceder únicamente a los datos necesarios para su función. Además, se definirán procesos específicos para capturar tanto el conocimiento tácito como el explícito, documentos y registros formales.

Las actividades necesarias para el diseño y definición de procesos se desarrollarán en reuniones mediante la plataforma Gather, facilitando una colaboración en tiempo real entre los participantes. En conjunto, este proyecto busca crear una base de conocimiento confiable y segura, que permita a la institución gestionar su información estratégica de manera estructurada y eficiente, cumpliendo con los estándares de seguridad exigidos en el sector financiero.

## **Justificación**

La creación de una base de conocimiento para una institución financiera es fundamental para mejorar la eficiencia en la gestión y protección de información crítica. En el sector financiero, la información manejada es sumamente sensible, abarcando desde datos financieros hasta normativas y procesos internos, por lo que es necesario implementar un sistema que permita el acceso seguro y adecuado. Esta propuesta se justifica debido a la importancia de contar con una estructura de gestión del conocimiento que no solo organice la información, sino que también garantice su seguridad mediante un diseño con controles de acceso estrictos, autenticación multifactor y supervisión de auditoría.

La plataforma Gather fue seleccionada para facilitar la colaboración en tiempo real, permitiendo al equipo trabajar de manera coordinada en la definición del diseño de la base de conocimiento y en los procesos de adquisición de conocimiento. Además, el uso de una herramienta de colaboración asegura que el desarrollo de la base de conocimiento sea dinámico y adaptado a las necesidades de seguridad y eficiencia de la institución.

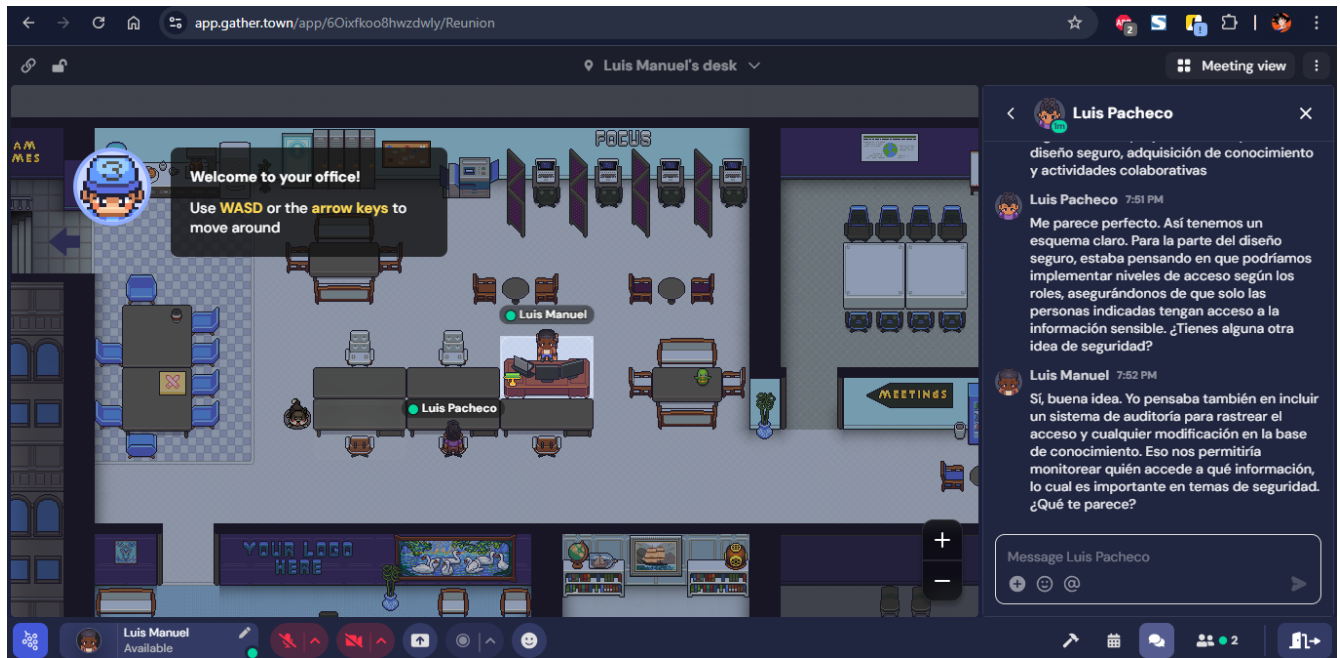
Este proyecto, por lo tanto, se justifica en la necesidad de una solución que no solo proteja la información sensible, sino que también permita mejorar la toma de decisiones y el aprovechamiento del conocimiento organizacional en un entorno controlado y confiable.

## Desarrollo

- **Reunión**

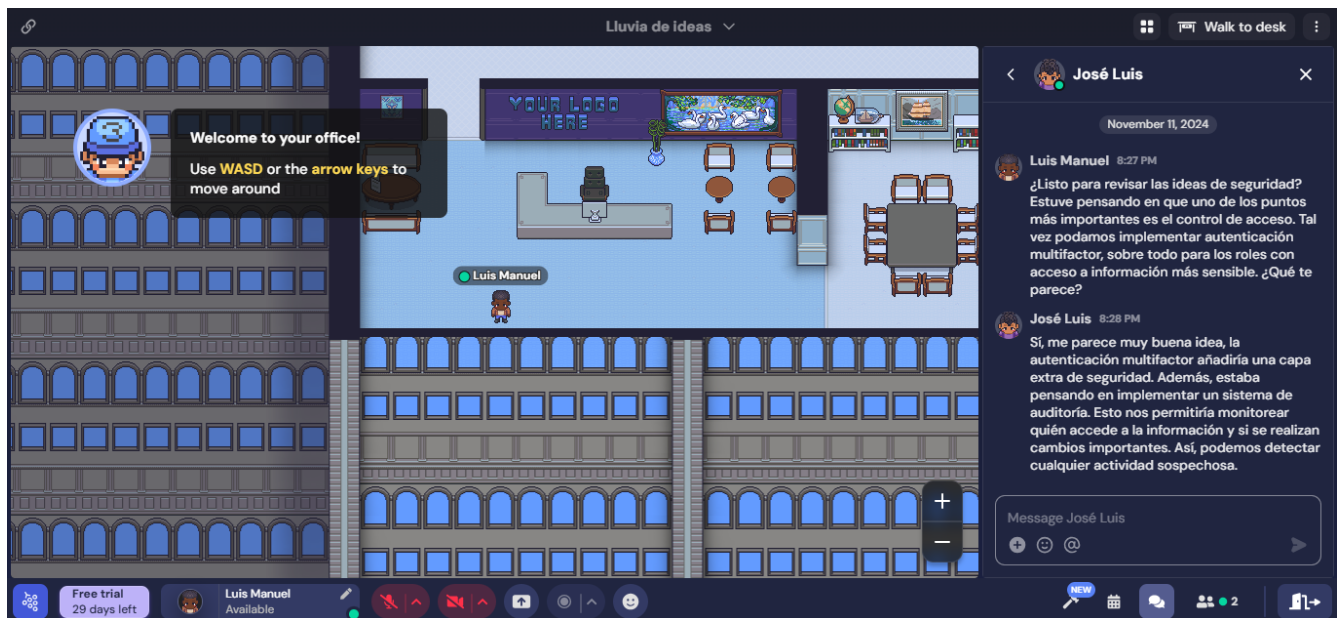
En la reunión inicial del proyecto, ambos miembros del equipo nos reunimos virtualmente en Gather para establecer los objetivos y dividir responsabilidades. Durante la sesión, discutimos la importancia de un diseño seguro para la base de conocimiento de la institución financiera, proponiendo medidas como el control de acceso por roles y el registro de auditorías. También definimos los procesos de adquisición de conocimiento (interno y externo, tácito y explícito) y asignamos tareas: uno de los miembros documentará el diseño seguro, mientras que el otro desarrollará los procesos de adquisición. Finalmente, acordamos una próxima reunión en tres días para revisar el avance.





- **Escenarios de colaboración**

Durante la sesión de lluvia de ideas, utilizamos Gather para discutir y proponer diferentes medidas de seguridad que fortalecerían el diseño de la base de conocimiento para la institución financiera. Cada integrante aportó ideas específicas: se sugirieron métodos como la autenticación multifactor, un sistema de auditoría de accesos, y permisos basados en roles, asegurando que cada usuario solo tenga acceso a la información que necesita. Además, consideramos la importancia de implementar políticas de caducidad de contraseñas y de ofrecer capacitación a los usuarios para reducir riesgos de seguridad. Estas ideas sentaron la base para un diseño enfocado en la protección y control de acceso de la información.





🔗

🔔

📍 José Luis's desk

Meeting view

🔍

👤 Luis Manuel

✕

👤 Luis Manuel 8:27 PM

¿Listo para revisar las ideas de seguridad? Estuve pensando en que uno de los puntos más importantes es el control de acceso. Tal vez podamos implementar autenticación multifactor, sobre todo para los roles con acceso a información más sensible. ¿Qué te parece?

👤 José Luis 8:28 PM

Si, me parece muy buena idea, la autenticación multifactor añadiría una capa extra de seguridad. Además, estaba pensando en implementar un sistema de auditoría. Esto nos permitiría monitorear quién accede a la información y si se realizan cambios importantes. Así, podemos detectar cualquier actividad sospechosa.

Message Luis Manuel

+

😊

@

➤

👤 José Luis Available

🔴

🔴

🔴

📷

🔊

🔇

😊

🔗

📅

💬

👥 2

🔖

🔗

🔔

📍 José Luis's desk

Meeting view

🔍

👤 Luis Manuel

✕

multifactor, y el sistema de auditoría. Puedo hacer un resumen claro para que se vea la estructura de seguridad que propusimos.

👤 Luis Manuel 8:40 PM

Perfecto. Y mientras tú documentas los puntos, yo me puedo enfocar en crear un esquema visual. Algo como un diagrama que muestre los niveles de acceso y los flujos de seguridad, para complementar tu documentación. Así, la entrega tendrá tanto el texto como una representación gráfica.

👤 José Luis 8:41 PM

Me parece muy bien. Así cubrimos tanto la explicación detallada como el esquema visual. ¿Qué te parece si en nuestra próxima reunión revisamos el esquema y la documentación juntos para asegurarnos de que todo esté alineado?

Message Luis Manuel

+

😊

@

➤

👤 José Luis Available

🔴

🔴

🔴

📷

🔊

🔇

😊

🔗

📅

💬

👥 2

🔖

- **Diseño de la base de conocimiento y Procesos de adquisición de conocimiento**

El diseño de la base de conocimiento de esta institución financiera se centra en la protección de información crítica mediante un marco de seguridad robusto y prácticas de control de acceso estrictas. Considerando la naturaleza de la información financiera y la necesidad de confidencialidad, integridad y disponibilidad, se han adoptado las siguientes medidas, desarrolladas a partir de una investigación exhaustiva de los estándares de seguridad más efectivos y apropiados para el sector financiero.

#### 1. Autenticación Multifactor (MFA)

La autenticación multifactor es una barrera de seguridad avanzada que combina varios factores de autenticación, como una contraseña y un código de verificación en un dispositivo móvil, para garantizar la identidad del usuario. Esta medida reduce significativamente los riesgos de accesos no autorizados, especialmente frente a ataques de ingeniería social y suplantación de identidad, problemas frecuentes en el sector financiero. La autenticación multifactor se complementará con:

Requerimientos de complejidad de contraseñas: Cada usuario deberá crear una contraseña que cumpla con altos estándares de complejidad, incluyendo caracteres especiales, mayúsculas, minúsculas y números.

Autenticación continua para roles críticos: Para usuarios en roles de alta responsabilidad o acceso a datos sensibles, se utilizará la autenticación multifactor en intervalos regulares y bajo contextos de sesión específicos, como al acceder a secciones de información de alto impacto o realizar operaciones de edición.

## 2. Sistema de Auditoría y Registro de Accesos

Para mantener un control riguroso y una trazabilidad precisa de todas las actividades dentro de la base de conocimiento, se ha integrado un sistema de auditoría automatizado. Este sistema tiene la capacidad de generar y almacenar registros detallados de cada actividad realizada por los usuarios, lo cual facilita la detección temprana de actividades sospechosas y asegura una alta visibilidad del uso de la plataforma. Los registros incluyen:

Historial de accesos, modificaciones y eliminaciones de contenido: Cada acción en la base de conocimiento queda registrada con la información de usuario, marca de tiempo y detalles de los cambios realizados.

Alertas de actividad sospechosa: El sistema enviará notificaciones inmediatas al equipo de seguridad cuando detecte patrones inusuales, como múltiples intentos fallidos de inicio de sesión, intentos de acceso fuera del horario laboral o desde ubicaciones no habituales.

Conservación de registros de auditoría: Los registros de acceso serán conservados y almacenados en un sistema encriptado, cumpliendo con las normativas de seguridad de la institución y garantizando su disponibilidad para auditorías internas o externas.

### 3. Control de Acceso Basado en Roles (RBAC)

Para minimizar el riesgo de exposición de datos sensibles, la base de conocimiento utiliza un modelo de control de acceso basado en roles (RBAC) que segmenta la información según los requisitos de cada puesto. Este diseño permite a cada usuario acceder únicamente a la información que corresponde a sus responsabilidades y funciones, adoptando así un esquema de “privilegios mínimos.” La estructura se detalla de la siguiente forma:

**Acceso General:** Usuarios con roles operativos y de consulta tienen acceso a información general y material de apoyo, excluyendo datos sensibles o estratégicos.

**Acceso Intermedio:** Usuarios en roles de liderazgo tienen acceso a información adicional y pueden editar o añadir contenido específico, pero sin permisos para acceder a datos financieros sensibles.

**Acceso Completo (Administradores):** Solo los administradores y el equipo de seguridad tienen acceso completo, incluyendo configuraciones de seguridad y módulos de auditoría. Este acceso se gestiona bajo políticas de revisión periódica para asegurar que solo los roles autorizados mantengan estos permisos.

#### 4. Política de Caducidad y Gestión de Contraseñas

Una política estricta de caducidad de contraseñas ha sido implementada para mitigar los riesgos asociados con credenciales obsoletas o comprometidas. Esta política exige a los usuarios cambiar sus contraseñas de forma regular y prohíbe el uso de contraseñas previamente utilizadas. Además, se adoptarán medidas como:

Notificaciones automáticas de cambio de contraseña: Los usuarios recibirán recordatorios para actualizar sus contraseñas antes de que expiren, evitando interrupciones en el acceso.

Validación de contraseñas en tiempo real: Las nuevas contraseñas se evaluarán en tiempo real para asegurar que cumplen con los estándares de seguridad exigidos por la institución, evitando combinaciones débiles o fáciles de adivinar.

#### 5. Capacitación Continua en Seguridad y Conciencia del Usuario

Dado que los errores humanos son una de las principales causas de incidentes de seguridad, se estableció un programa de capacitación continuo para asegurar que los usuarios comprendan y apliquen buenas prácticas de seguridad. Esta capacitación incluye:

Sesiones periódicas de formación en seguridad: Se abordarán temas como la detección de intentos de phishing, la gestión responsable de la información y los riesgos de compartir datos sensibles.

Actualización en prácticas de seguridad: Ante nuevas amenazas o actualizaciones de seguridad, se realizarán sesiones informativas para mantener a los usuarios actualizados y preparados.

Evaluaciones periódicas de seguridad: Los usuarios deberán completar cuestionarios breves para asegurar que comprenden los protocolos y se mantengan alerta sobre sus responsabilidades en la seguridad de la información.


## 6. Representación Visual y Documentación del Diseño de Seguridad

Para complementar el diseño de la base de conocimiento y asegurar una fácil comprensión por parte de los usuarios, se incluirá un esquema visual detallado. Este esquema representará:

Niveles de acceso y flujo de información: Se mostrará cómo está segmentado el acceso en base a roles, indicando las capas de protección para información sensible.


Puntos de control de seguridad: Se destacarán las barreras de seguridad, incluyendo autenticación multifactor, auditoría y control de acceso por roles, para una comprensión clara de las zonas seguras.

Flujos de intervención: El esquema también ilustrará cómo y cuándo se activan los controles de seguridad, como auditorías y alertas en caso de actividad inusual.



¿Cómo este diseño fomenta la seguridad de la información?

Este diseño fomenta la seguridad de la información al implementar un sistema de control de acceso basado en roles específicos, lo que asegura que cada usuario solo pueda acceder a la información necesaria para sus tareas, limitando la exposición de datos sensibles. La autenticación multifactor refuerza esta seguridad, ya que los usuarios deben pasar por varias capas de verificación antes de obtener acceso, reduciendo el riesgo de accesos no autorizados. Además, se integra un esquema de auditoría continuo que permite monitorear todas las actividades dentro de la base de conocimiento, identificando patrones o accesos sospechosos en tiempo real.



Esta tabla organiza los elementos de conocimiento según su origen interno o externo y su naturaleza tácito o explícito, destacando los distintos tipos de información relevantes para la gestión y seguridad de la base de conocimiento en la institución financiera.

Interno o Externo	Tácito o Explícito
<ul style="list-style-type: none"><li>• Experiencia en la gestión segura de información dentro de la institución.</li><li>• Procedimientos internos para verificar identidad y acceso.</li><li>• Prácticas de seguridad observadas en otras instituciones financieras.</li><li>• Habilidades específicas en el uso de herramientas de colaboración.</li><li>• Consultoría y asesoramiento de expertos externos en ciberseguridad.</li></ul>	<ul style="list-style-type: none"><li>• Documentación detallada de políticas y procedimientos de seguridad.</li><li>• Manuales de usuario y guías para el personal.</li><li>• Normativas y estándares de seguridad nacionales e internacionales.</li><li>• Procedimientos escritos sobre autenticación multifactor y auditoría.</li><li>• Protocolos documentados de respuesta ante incidentes y reportes de auditoría.</li></ul>



## Conclusión

El desarrollo de una base de conocimiento robusta y segura es esencial para mejorar la gestión de la información dentro de una institución financiera. Este proyecto responde a la necesidad de salvaguardar datos sensibles, al tiempo que optimiza el acceso y la utilización del conocimiento relevante, lo cual favorece tanto la eficiencia interna como el cumplimiento de las normativas de seguridad. Utilizar una plataforma como Gather para trabajar en conjunto y crear el diseño de la base de conocimiento permite una colaboración ágil y estructurada, donde los equipos pueden compartir sus experiencias y conocimientos de manera controlada.

La implementación de procesos de adquisición de conocimiento, tanto de fuentes internas como externas, así como de tipo tácito y explícito, asegura que la información esté organizada y disponible solo para los usuarios autorizados. La integración de medidas de seguridad, como la autenticación multifactor y los controles de acceso basados en roles, junto con una auditoría constante de las acciones realizadas, garantiza la protección de la información.

Todo esto no solo optimiza la gestión del conocimiento, sino que también refuerza la seguridad y fiabilidad de la institución financiera, permitiendo operar de manera segura y conforme a los estándares del sector.

## Referencias

Guía de supervivencia para la seguridad de los datos. (n.d.). Provident.bank. Retrieved November 13, 2024, from <https://www.provident.bank/es/educaci%C3%B3n-y-recomendaciones/empresarial/preg%C3%BAnte-al-experto-gu%C3%ADa-de-supervivencia-para-la-seguridad-de-los-datos>



**Enlace Github**