Automatización de la gestión de accesos y alertas de seguridad de acuerdo con la clasificación de la información publicada en la plataforma Business Intelligence

Aileen Correa Ochoa, Carlos Alberto López Prada, Oscar Enrique García Mesa
Maestría en Seguridad de la Información y Maestría en Tecnologías de la Información para el Negocio
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes Bogotá, Colombia
Noviembre de 2021

1. Introducción

En el 2019 se creó una dependencia perteneciente a una Entidad del gobierno, encargada de monitorear fuentes de datos, hacer analítica y levantar alertas tempranas que permiten disminuir y evitar la pérdida de recursos públicos.

Con la conformación de esta nueva área, fue necesario introducir grandes cambios, entre ellos, estructurar y organizar la gestión del control de acceso a los más de 135 tableros de uso interno con información de alertas presupuestales, resultados de modelos de detección de detrimento patrimonial y seguimientos al manejo presupuestal de la nación. Información que en su mayoría es de carácter sensible y confidencial.

El procedimiento existente de control de acceso a la información presenta algunas deficiencias, entre las cuales están, la asignación manual de permisos para los más de mil funcionarios, la ausencia de una definición clara de perfiles, y niveles de acceso de acuerdo con las funciones y el registro manual de estos permisos asignados en un archivo de Excel; dejando una alta probabilidad de riesgo de errores humanos, pérdida de información, daño del archivo, generación de diferentes versiones o descuidos al registrarla o guardarla.

Así mismo, el tiempo requerido para la asignación de permisos y el registro de estos, es una tarea repetitiva y dispendiosa que consume gran parte del tiempo del responsable y que, debido a la importancia, no puede ser delegada a otra persona por su criticidad. La complejidad de este proceso y las tareas manuales que se realizan, pueden ocasionar inconsistencias y posible discontinuidad en el momento en que se presente una ausencia o cambio de responsable, dado que actualmente no cuenta con la suficiente estructuración y madurez.

1.1. Análisis y Diseño de la solución

Para la solución propuesta se diseño el proceso de gestión de usuarios, clasificación de la información y la integración con la arquitectura de TI de la organización a través de:

- Análisis y clasificación de los niveles de confidencialidad de la información
- Integración del Directorio Activo para la gestión automática de usuario con acceso a los tableros de Power Bi.
- Generación de alertas de seguridad para la creación, modificación y eliminación de usuarios.
- Diseño de alertas tempranas que identifiquen los limites preestablecidos en los datos de los tableros.

Teniendo en cuenta el organigrama de la Entidad, se presenta a continuación un diseño de la solución, en donde se evidencia el esquema de orden para las diferentes dependencias dentro de la Entidad, partiendo de la administración de recursos tecnológicos que integran herramientas de automatización y las medidas correspondientes de seguridad que garanticen la integridad en el desarrollo de las actividades.

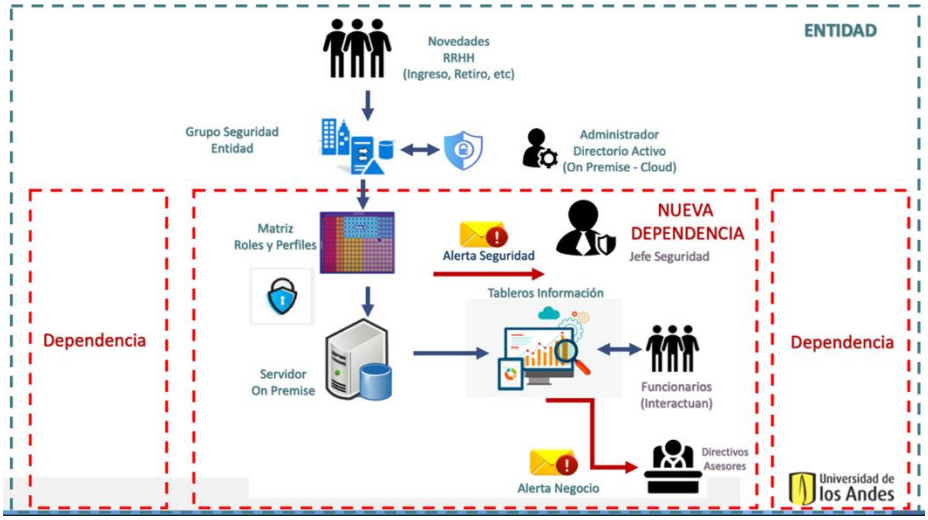

Figura 1. Diseño de la solución

Las novedades como ingresos, cambios de dependencia o cargos y los retiros, que son reportadas por el grupo de Recursos Humanos de la Entidad, y comunicados a la oficina de sistemas; se ven reflejados en el Directorio Activo (On Premise y Cloud). En el Directorio Activo se establecen Grupos de Seguridad acordes con las directrices del Jefe de Seguridad de la nueva dependencia y el administrador de la oficina de sistemas de la Entidad, las cuales quedan plasmadas en la Matriz de Roles y Perfiles. Con base en dicha matriz, se gestiona el correspondiente acceso a los tableros de información, los cuales están clasificados de acuerdo con el nivel de confidencialidad de ésta.

1.2 Arquitectura y Componentes de Sistema

Teniendo en cuenta el organigrama de la Entidad, se presenta a continuación un diseño de la solución, en donde se evidencia el esquema de orden para las diferentes dependencias internas, partiendo de la administración de recursos tecnológicos que integran herramientas de automatización y las medidas correspondientes de seguridad que garanticen la integridad en el desarrollo del proyecto.

Las novedades como ingresos, cambios de dependencia o cargos y los retiros de funcionarios se ven reflejados en el Directorio Activo (On Premise y Cloud), donde previamente fueron establecidos Grupos de Seguridad acordes con las directrices del Jefe de Seguridad de la dependencia y el administrador de la oficina de sistemas, las cuales quedan plasmadas en la Matriz de Roles y Perfiles. Con base en dicha matriz, se gestiona el correspondiente acceso a los tableros de información, los cuales están clasificados de acuerdo con el nivel de confidencialidad de ésta.

Se presentan las diferentes aplicaciones que mejor se acoplan con el diseño de la solución y con las cuales cuenta la Entidad en los entornos On Premise y Cloud para el desarrollo del proyecto, en este caso, y para facilidad de integración y administración de las diferentes plataformas se escogen las herramientas de Microsoft y su plataforma Cloud Azure:

- Directorio Activo On Premise y Microsoft Azure Active Directory Cloud
- Servidor Dell PowerEdge R470 On Premise
- Plataforma Microsoft Power BI Report Server On Premise (Tableros y Reportes)
- Plataforma Microsoft SQL Server – Bases datos Power Bi (On Premise)
- Entorno Microsoft Azure Power Automate (Cloud)

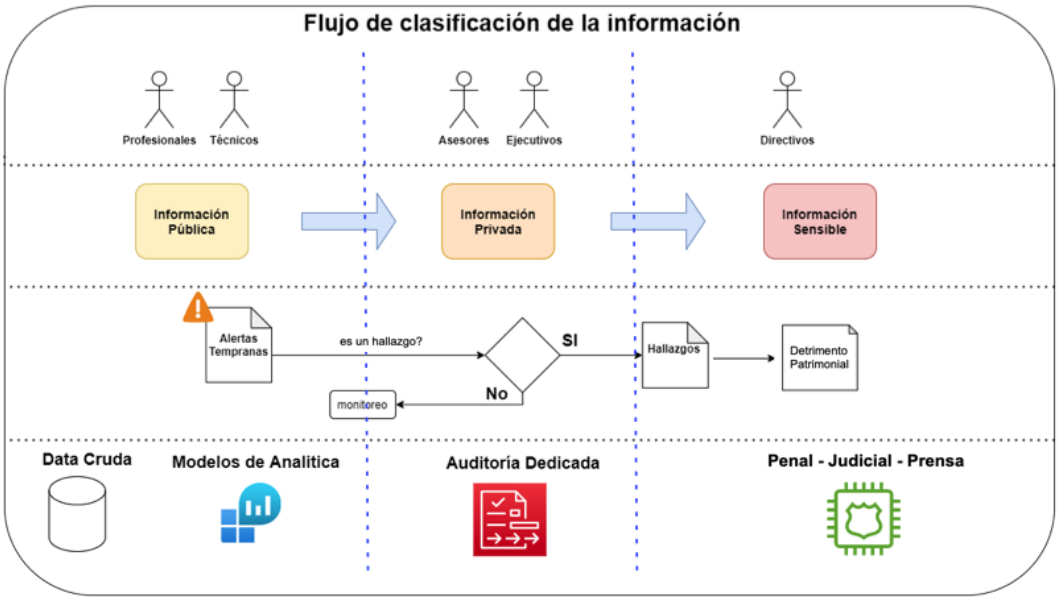

Figura 2. Flujo de clasificación de la información

2. Implementación

Para el desarrollo de este proyecto se realizó el análisis y la clasificación de los niveles de confidencialidad de la información publicada en los tableros, teniendo en cuenta el tipo de información que maneja la Entidad y las responsabilidades por cargo de cada uno de sus funcionarios en las diferentes dependencias. A continuación, se presenta la matriz de clasificación de la información por cargo, la clasificación de la sensibilidad y los criterios estipulados por la dependencia la clasificación de responsabilidades asociadas al manejo de la información de acuerdo con el cargo y tareas contempladas dentro de Power Bi.

	Clasificación de la Información por Cargo		
	Sensible (cuando presenta un nivel mayor de confidencialidad).	**Privada** (nivel más bajo de confidencialidad)	**Público** (cuando la información es accesible a todo el público)
Directivo	X	X	X
Asesor		X	X
Ejecutivo		X	X
Profesional		X	X
Técnico			X
Asistencial			X
JEFE SEGURIDAD	-	-	-

Figura 3. Matriz de la clasificación de la información de los tableros de acuerdo con el cargo del funcionario

Diseño de una matriz de roles y perfiles para la gestión de acceso de usuarios a los más de 135 tableros en Power Bi basados en los tipos de acceso que la plataforma permite asignar y el nivel de acceso requerida de acuerdo con el cargo:

Tipo de acceso a Workspaces de Power Bi	
ROL	Descripción
Admin	Privilegios de administración de la plataforma
Member	Crear, editar Workspace, incluyendo los tableros y reportes contenidos
Contributor	Crear, editar, publicar información, tableros y reportes, clasificarlos según su contenido y agruparlos por sectores
Viewer	Visualizar los datos presentados en los tableros, dependiendo del sector y del nivel de clasificación autorizado, compartir, generar reportes, descargar y exportar excel.

Rol	Tipo de accesos en los Workspaces de Power - Bi			
	Admin	Member	Contributor	Viewer
Jefe de seguridad	X			
Directivo			X	
Asesor		X		
Ejecutivo			X	
Profesional			X	
Técnico		X		
Asistencial				X

Figura 4. Matriz de Tipos de acceso Workspace de Power Bi y asignación de accesos de acuerdo con el cargo

2.1 Arquitectura y Componentes de Sistema

Los lineamientos de arquitectura de aplicaciones aceleran la selección de alternativas de tecnología. Se debe establecer un plan de emisión de lineamientos priorizado por relevancia de las aplicaciones para cumplir las metas de negocio. A continuación, se presentan las diferentes aplicaciones que mejor se acoplan con el diseño de la solución y con las cuales cuenta la Entidad en entorno On Premise y Cloud para el desarrollo del proyecto, en este caso, y para facilidad de integración y administración de las diferentes plataformas se escogen las herramientas de Microsoft y su plataforma Cloud Azure:

- Directorio Activo On Premise y Microsoft Azure Active Directory Cloud
- Servidor Dell PowerEdge R470 On Premise
- Plataforma Microsoft Power BI Report Server On Premise (Tableros y Reportes)
- Plataforma Microsoft SQL Server – Bases datos Power Bi (On Premise)
- Entorno Microsoft Azure Power Automate (Cloud)

2.2 Seguridad

Al implementar la integración entre el Directorio Activo en Azure y Power Bi Cloud, se optimizaron los siguientes aspectos de seguridad:

A nivel de proceso:

- Administración de usuarios de Power Bi desde un sistema centralizado de la organización (**AD**, Directorio Activo).
- Simplificar la gestión de accesos a través de la agrupación de usuarios y tableros.
- Monitoreo automatizado de los indicadores del uso de bienes públicos.

A nivel de seguridad:

- Clasificación de la información y definición de los niveles de confidencialidad.
- Activación del método de validación de identidad adicional (Multi Factor Authenticator)
- Logs de auditoría que facilitan el seguimiento y detección de inconsistencias.
- Envío de alertas de seguridad automáticas a través del correo electrónico.

Por otro lado, la protección de identidades (Azure AD Identity Protection) es una característica de la versión Premium que permite:

- Detectar identidades vulnerables.
- Respuestas automáticas a posibles amenazas a las identidades.
- Investigar y resolver incidentes relacionados con las identidades.

Por último, la administración de cuentas con privilegios (Azure AD Privileged Identity Management) es otra característica de Azure AD Premium que ayuda a gestionar y proteger las credenciales de administrador, monitorizando las actividades de los administradores y restringiendo el acceso a los recurso

3. Prueba de Concepto (POC)

Realizar la integración entre el directorio activo de la Entidad con la base de datos de la plataforma de Business Intelligence para la asignación automática de roles y perfiles a los tableros de la nueva dependencia.

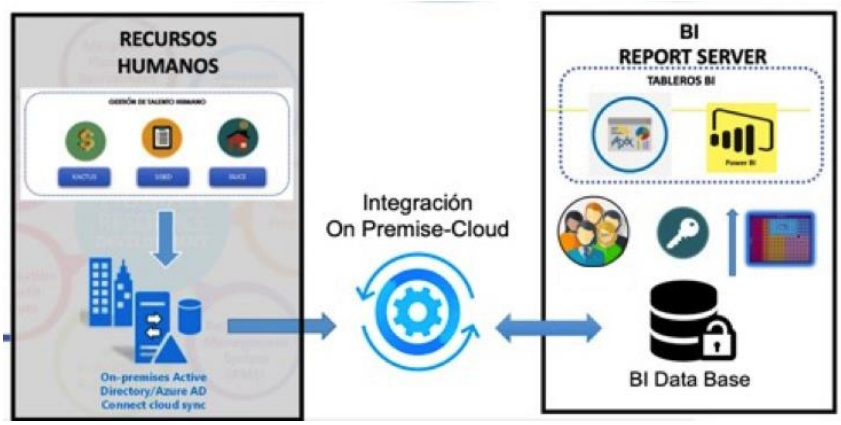

Figura 5. Integración del Directorio Activo con la plataforma de Business Intelligence

Mediante el uso de los grupos de seguridad gestionados en el Directorio Activo, por el Administrador de infraestructura y el Jefe de Seguridad, se propone realizar la automatización de usuarios (CRUD) entre el Directorio Activo y la plataforma de Business Intelligence, con el fin de otorgar accesos a los diferentes tableros de la nueva dependencia de acuerdo a la clasificación de la información, cargos de usuarios y tipo de acceso que debe tener a cada uno de estos, según la responsabilidades de cada cargo, lo cual se encuentra definido en la Matriz de Clasificación de la información y Matriz de Roles y Permisos diseñadas para este proyecto.

Por otro lado, la protección de identidades (Azure AD Identity Protection) es una característica de la versión Premium que permite:

- Detectar identidades vulnerables.
- respuestas automáticas a posibles amenazas a las identidades.
- Investigar y resolver incidentes relacionados con las identidades.

Por último, la administración de cuentas con privilegios (Azure AD Privileged Identity Management) es otra característica de Azure AD Premium que ayuda a gestionar y proteger las credenciales de administrador, monitorizando las actividades de los administradores y restringiendo el acceso a los recursos.

3.1 Gestión de accesos a Tableros de Power Bi para usuarios

El Directorio Activo de la Entidad refleja las novedades reportadas por Recursos Humanos de los empleados que ingresan, cambian de cargo o salen de la Entidad, a través de la integración entre el directorio activo y Power Bi Report Server se sincronizan los diferentes roles y perfiles, gestionando el acceso a los tableros de información de la nueva dependencia.

A través de *Microsoft Azure Active Directory* se sincronizan los cambios que se hacen en el Directorio Activo On Premise de la Entidad, de esta forma se puede administrar de manera fácil y transparente los recursos tecnológicos tanto On Premise como Cloud de la Entidad.

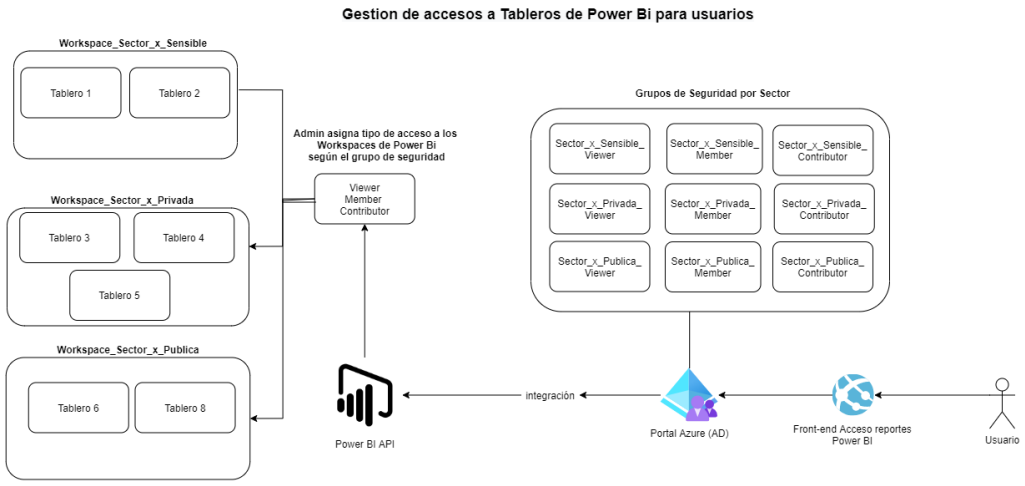

Figura 6. Diagrama de gestión de acceso en AD y Power Bi – Rol Usuario

Con el fin de centralizar la administración de los accesos otorgados a los tableros de Power Bi, se propone realizar la administración a través del directorio activo. Como base fundamental, todo usuario hace parte de una dependencia dentro de la Entidad y su respectivo cargo, con los cuales se definen los accesos que este deberá tener de acuerdo con la matriz de roles y perfiles y la matriz de clasificación de la información.

Una vez el administrador de infraestructura haya creado el usuario en el Directorio Activo, el Jefe de Seguridad podrá agregar, eliminar y cambiar a los usuarios en los grupos de seguridad definidos para Power Bi. Restringiendo el acceso a los diferentes tableros según sea el caso.

3.2 Grupos de seguridad

Siguiendo el lineamento de la Matriz de Roles y Perfiles y la Matriz de clasificación de la información, se propone crear (9) grupos de seguridad para cada sector económico de la compañía definidos de la siguiente manera:

Sector Económico + Nivel de clasificación de información + Tipo acceso en Power Bi

- Power_BI_Workspace_SectorX_Privada_Contributor
- Power_BI_Workspace_SectorX_Privada_Member
- Power_BI_Workspace_SectorX_Privada_Viewer
- Power_BI_Workspace_SectorX_Publica_Contributor
- Power_BI_Workspace_SectorX_Publica_Member
- Power_BI_Workspace_SectorX_Publica_Viewer
- Power_BI_Workspace_SectorX_Sensible_Contributor

- Power_BI_Workspace_SectorX_Sensible_Member
- Power_BI_Workspace_SectorX_Sensible_Viewer

Los administradores se gestionarán a través del grupo de seguridad

- Power_BI_Admin

Todo usuario que sea parte de este grupo tendrá acceso a todos los Workspace dentro de Power Bi, sin importar la clasificación de los tableros.

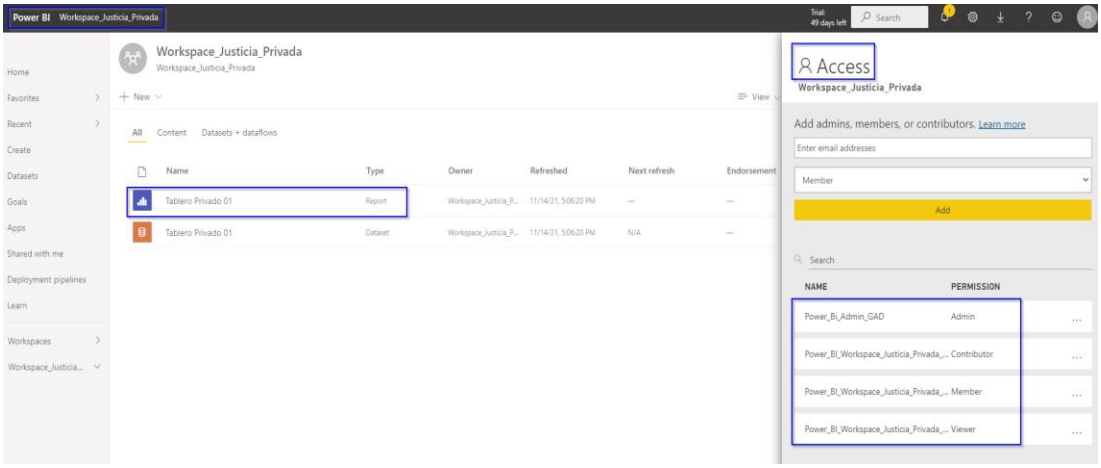

Figura 7. Accesos asignados al Workspace a través del uso de grupos de seguridad

Los grupos se usan para recopilar cuentas de usuario, cuentas de equipo y otros grupos en unidades administrables. Trabajar con grupos en lugar de con usuarios individuales ayuda a simplificar el mantenimiento y la administración de la red.

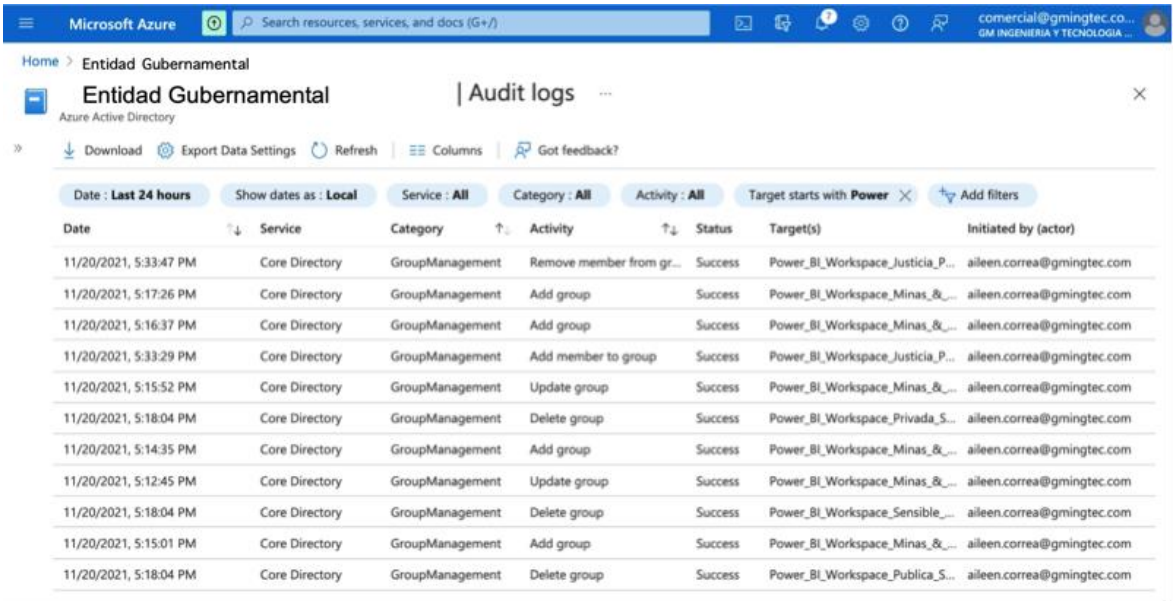

Figura 8. Logs de auditoria de usuarios y grupos de seguridad en el Directorio Activo

Para cada workspace se debe agregar los usuarios que tendrán acceso. En las pruebas POC se logró optimizar este proceso de asignación de permisos y evitar realizar la asignación individual de usuarios, mediante el uso de grupos del AD.

Power Bi Report Server permite administrar, gestionar, publicar y crear tableros (utilizando Power Bi Desktop) a los cuales van a acceder los directivos, ejecutivos, empleados profesionales y técnicos de la nueva dependencia. Estos informes son enriquecidos e interactivos, donde se tiene la posibilidad de escalar el acceso y la seguridad hasta más de miles de usuarios, debido a que Power BI Report Server se puede integrar al directorio activo de la Entidad, tanto On Premise como Cloud.

Por otro lado, en la base de datos están contenidos los *logs* de accesos y el historial de los cambios en los permisos que se dan o van retirando a los usuarios, en esta base de datos se específica el nivel de acceso, el tablero correspondiente y las fechas en que se realizaron los cambios o ajustes.

Power Automate integra diferentes entornos tecnológicos con flujos de negocio y reglas de seguridad, basadas en políticas de la organización, de manera eficaz y automática, permitiendo generar notificaciones de creación, modificación y eliminación de usuarios, a través de email al jefe de seguridad de la nueva dependencia, teniendo en cuenta la matriz de roles y perfiles, quien valida el acceso del respectivo usuario. También permite notificar a través de correo electrónico, a los ejecutivos, asesores, directivos y contralores delegados de cada sector, las alertas tempranas que se generan después del cruce de bases y la analítica de datos que realizan los profesionales de la unidad de análisis de la nueva dependencia.

3.3 Alertas de seguridad:

Diseñar alertas de seguridad para la creación, modificación, eliminación de usuarios en los diferentes grupos de seguridad y la asignación de permisos a los tableros, basada en el análisis de los eventos del log de actividades de la plataforma de Business Intelligence, con el fin de que sean evaluadas por el Jefe de Seguridad.

La alerta de seguridad se genera de forma automática, mediante la construcción de un flujo y dirigiendo la atención del jefe de Seguridad hacia estas novedades para que pueda reaccionar e impedir el acceso, para los casos de un intento de acceso no autorizado, y poder identificar de manera rápida quien accedió, a donde y en qué momento, junto con otros detalles de cada evento. Con la implementación de alertas mediante notificaciones en tiempo real, se podrá disminuir el tiempo de respuesta a eventos, identificando de manera pronta los falsos positivos basado en el análisis de comportamientos de los usuarios.

Con los grupos de seguridad creados en el directorio activo y utilizando la herramienta Power Automate, se crea un flujo automatizado que permite crear alertas de seguridad sobre modificaciones o cambios en estos grupos.

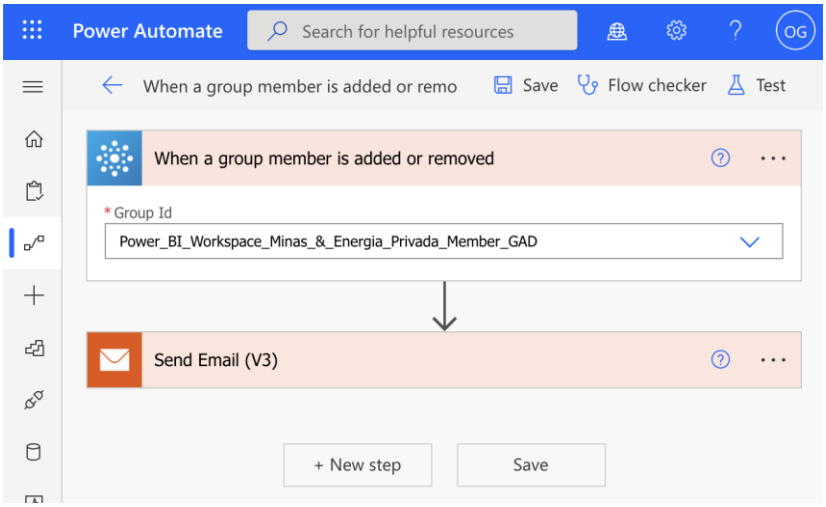

Figura 9. Flujo notificación seguridad Power Automate

Estas alertas son notificadas mediante correo electrónico al Jefe de Seguridad de la nueva dependencia, para que verifique y corrobore los cambios de adición, modificación o remoción de los funcionarios que tendrán acceso a los tableros de Power Bi, disminuyendo los tiempos de gestión, al tener información previa que le permita clasificar y analizar las alertas que merezcan atención prioritaria, lo que facilita una gestión automatizada y en tiempo real sobre el control de cambios de los usuarios.

Figura 10. Notificación de cambio en grupo de seguridad.

3.4 Alertas de Negocio

Basados en las consideraciones de las distintas dependencias, se establecen reglas de negocio tales como los topes de indicadores, métricas y validaciones presentadas en los tableros de Power Bi y en conjunto con un flujo lógico construido en Power Automate, permite notificar a los directivos y ejecutivos en aras de reforzar el proceso de auditoría.

Para establecer dichas alertas, se selecciona en Power Bi, el ítem que se desea monitorear, se agrega la regla correspondiente cómo que el valor del ítem supere un tope establecido por el directivo de la dependencia.

Figura 11. Tablero de la plataforma Business Intelligence

Para generar dichas alertas tempranas se genera un flujo automatizado de la plataforma Cloud que se activa al alcanzar o sobrepasar un límite en el tablero de la plataforma de Business Intelligence, tal como se ilustra en la figura 12.

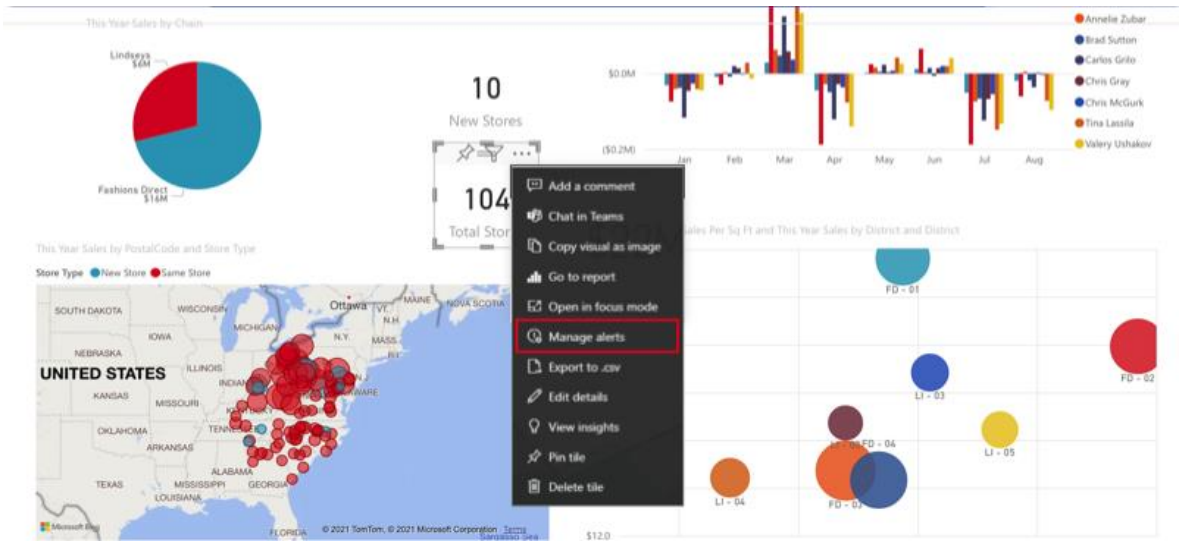

Figura 12. Establecer alertas en tablero Power Bi y Power Automate

Los flujos automatizados permiten generan alertas de seguridad y notificaciones de negocio, a través de scripts y pasos secuenciales de trabajo iniciados por cambios en un recurso On Premise o Cloud, o en un flujo de proceso de negocio que aplicarán cuando se modifiquen los datos en un tablero. Si la automatización se aplica mediante un flujo de trabajo en tiempo real, los cambios serán visibles inmediatamente para el usuario cuando se actualicen los datos del tablero o se agregue un usuario.

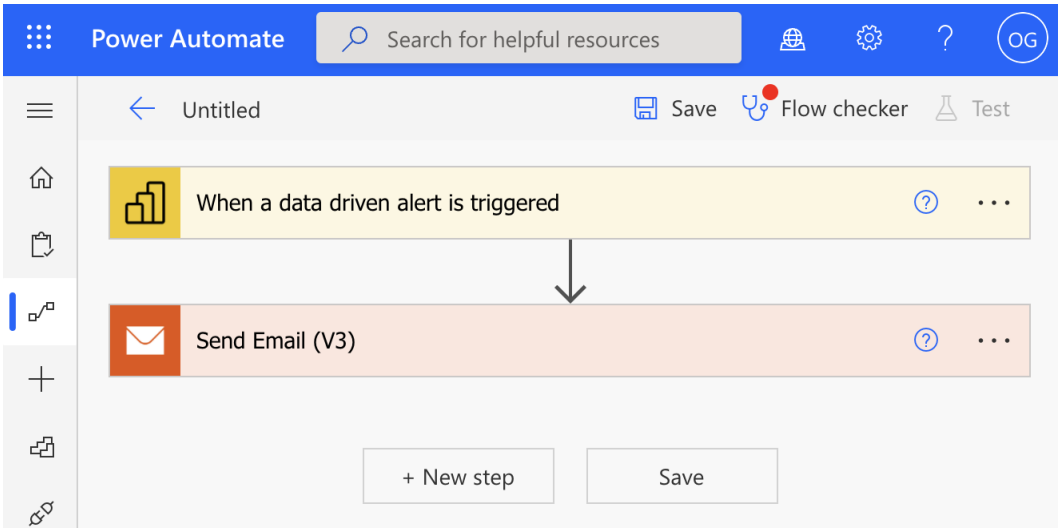

Figura 13. Flujo de notificación de alertas de negocio en Power Automate

4. Conclusiones

El proceso de gestión de accesos para los tableros de la nueva dependencia publicados en Power Bi, se ve optimizado a nivel de asignación, administración y seguridad con la implementación de las herramientas que ofrece Microsoft Azure debido a su fácil integración y adaptabilidad con todos los productos Microsoft 365.

La administración de los tableros se ve optimizada al implementar el esquema de Workspace, el cual permite agrupar los tableros con características comunes definidas por el administrador y gestionar los accesos de manera centralizada desde el Directorio Activo, esto evita la configuración individual de accesos a cada uno de los tableros que podría comprometer la seguridad de la información publicada.

Combinando los flujos automatizados que se hicieron con Power Automate y la plataforma de Business Intelligence, en este caso Power Bi, permite administrar de manera mucho más eficiente los accesos a los tableros de información, al igual que automatiza el registro y el historial de cambios o modificación de usuarios en la plataforma de Power BI. Por otro lado, permite agilizar la detección de nuevos usuarios que sean adicionados o removidos del entorno, a través de una notificación por correo electrónico al Jefe de Seguridad, dándole la oportunidad de validar la correcta asignación de los permisos.

Existe una reducción en aproximadamente el 75 % en las horas hombre (de 4 horas a 1 horas diarias), que se necesitan en la gestión de roles y perfiles de los funcionarios de la nueva dependencia y la Entidad, fortaleciendo la seguridad de la información que se despliega en los tableros de Power BI, al igual que se disminuye en gran medida las posibilidades del error humano.

5. Referencias

[1] Configure email notifications for issues in Azure Active Directory Domain Services

https://community.powerbi.com/t5/Community-Blog/Working-with-Power-BI-Gateway-logs/ba-p/1352383

[2] How to configure notifications and email templates in Azure API Management.

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/notifications

[3] Roles in the new workspaces in Power BI. https://docs.microsoft.com/en-us/power-bi/collaborate-share/service-roles-new-workspaces

[4] Integrate Power BI data alerts with Power Automate. https://docs.microsoft.com/en-us/power-bi/collaborate-share/service-flow-integration

[5] Share Power BI reports and dashboards with coworkers and others. https://docs.microsoft.com/en-us/power-bi/collaborate-share/service-share-dashboards

[6] The new workspace experience in Power BI. https://docs.microsoft.com/en-us/power-bi/collaborate-share/service-new-workspaces

[7] Seguridad y gobernanza en Azure AD. https://azure.microsoft.com/es-es/services/active-directory/security/