Julio Ernesto Alvarez Benitez
Firmado digitalmente por Julio Ernesto Alvarez Benitez
Fecha: 2025.08.19 10:50:33 -05'00'

El futuro digital es de todos
Gobierno de Colombia MinTIC

Reporte de Incidentes

Fecha del Reporte: 24/07/2025 10:09 a. m.

Datos de Contacto de la Entidad		
Nombre de la Entidad: Banco de la República		
Dirección: Carrera 7 #14-78 piso 7		**Sede: Principal**
Sector: Financiero	**Ciudad: Bogotá**	**Departamento: Bogotá D.C.**
Nombre de Quien Reporta: Elvira Marcela Guzmán Guzmán		
Cargo: Asesora Líder Ciberdefensa	**Número Contacto:** **Fijo: 3431111 Ext** Número de la extensión **Celular: 3002144500**	
Correo Electrónico: jalvarbe@banrep.gov.co		**Skype:** Escriba su usuario de Skype

Incidente	
Fecha y Hora del descubrimiento: 19/07/2025 12:25 p. m.	**Nombre de la Persona que Detectó el Incidente: Servicio MDR/SOC**
Fecha y Hora de Detección: 19/07/2025 5:21 p. m.	**Nombre del administrador del Activo Informático:** Escriba el nombre y apellidos de la persona que administra el activo informático – Servidor, DB, Aplicación, Portal, etc.
Descripción Detallada: Un acceso exitoso, no autorizado, fue detectado en la infraestructura de nube del Banco de la República el 19 de julio de 2025 a las 12:25pm. Este incidente involucró el abuso de un secreto sobre Microsoft Graph, asociado a una consulta específica dirigida a obtener información de nombre de cuentas y nombres de usuario en Azure Active Directory.	
Método de Detección: La actividad fue identificada como una anomalía por la plataforma de correlación y fue analizada por el servicio MDR/SOC externo quienes determina el acceso desde una dirección IP asociada con un nodo TOR, y es reportada al equipo de operaciones del Banco.	
Acciones Realizadas:	

Para la gestión de este incidente se tomaron una serie de medidas de investigación y contención, tanto con recursos internos del Banco como con el apoyo de entidades externas tipo Incident Response Retainer. Algunas de estas medidas son:
- Bloqueo de la dirección origen
- Reset de usuarios
- Aislamiento y escaneos de dispositivos
- Borrado de la aplicación y su secreto
- Validación de actividad maliciosa potencialmente asociada a la aplicación y al secreto abusados
- Toma de imágenes forenses y análisis de las mismas
- Búsquedas de compromiso y fuga del secreto en toda nuestra infraestructura
- Renovación de los secretos de las demás aplicaciones registradas en Microsoft Graph, con acceso al directorio activo.
- Monitoreo de deep y dark web

Acciones Pendientes:

Clasificación del Incidente: Seleccione la clase y tipo de incidente.

Malware: Elija un elemento.
Disponibilidad: Elija un elemento.
Obtención de Información: Elija un elemento.
Intrusiones: Elija un elemento.
Compromiso de Información: **Acceso no autorizado a información**
Fraude: Elija un elemento.
Contenido Abusivo: Elija un elemento.
Política de Seguridad: **Acceso a servicios no autorizados**
Otros:
Escriba la clasificación del incidente, si no se encuentra en las listas desplegables

La respuesta al incidente fue efectiva: **SI**	**Duración del Incidente: Días** **Horas** **Minutos 10**

Se Identifico el Responsable:	**Nombre:** Escriba el nombre y apellidos de la persona responsable	**Área:** Escriba el nombre del área, al cual pertenece la persona responsable
○ SI ◉ NO		

Hardware y Software Afectado

Servicios Afectados: ☐ Misionales ☐ Estratégicos ☐ Financieros ☐ Tecnológico ☐ Soporte y Mejora

☐ Servidor ☐ PC ☐ Portátil ☐ BD ☐ Portal WEB ☐ Aplicación ☐ Correo ☐ Equipo Activo ☐ Otros
Descripción Detallada del Activo o Servicio Afectado: El activo comprometido corresponde al servicio de Microsoft Graph, una interfaz de programación de aplicaciones (API) que permite acceder a múltiples recursos de la plataforma Microsoft 365, incluyendo información de Azure Active Directory (AD).

Debido al Incidente:	Alguien no autorizado tuvo acceso a la información: SI
	Se ha impedido a algún usuario el acceso a la información: NO
	Se ha borrado, modificado y eliminado alguna información: NO

Impacto del incidente: ☐ Financiero ☐ Reputacional ☐ Operacional ☐ Legal

Causa Raíz:
La causa raíz más probable de este incidente es una exposición involuntaria de credenciales de un service principal

Realizo Plan de Mejoramiento: ◉ SI ○ NO

Acciones Planificas para Solución Causa Raíz:

- Evitar el almacenamiento inseguro de credenciales
- Reforzar la protección de service principals
- Monitoreo proactivo de geolocalización y comportamiento
- Concientización y capacitación del personal técnico

Lecciones Aprendidas:
La operacionalización de los servicios en nube trae consigo retos adicionales para el monitoreo de todos los puntos de acceso a estos servicios e infraestructura.

Después de realizar la contención y actividades de mitigación el incidente se encuentra: Cerrado	**El incidente ya se había presentado:** ○ SI ◉ NO

Otros:

IoC

185.40.4.132

Contáctanos

Si tienes alguna consulta técnica, comunicarse con CSIRT Gobierno a través de los siguientes canales:

Bogotá: 601 344 22 22 Línea Gratuita Nacional: 018000952525 Op. 2

csirtgob@mintic.gov.co