Medellín, 8 de agosto de 2025

Señores,
Distrito Especial de Medellín
Atn. Santiago Restrepo Arroyave
Secretario de Despacho
Medellín, Colombia

REFERENCIA: Contrato 02027501 – 2024
TEMA: Incidente eliminación de cuenta admindevops
RADICADO: DM-TIGO-SAMI- 014-08082025

Respetados Señores,

En atención al oficio recibido el día 31 de julio de 2025 con el radicado número 202530355720 y frente a la preocupación manifestada, aclaramos que el incidente correspondió a la eliminación no intencionada de la cuenta *admindevops@medellin.gov.co*, ocurrida durante una rutina de depuración de usuarios en Active Directory y su sincronización con Entra ID. Como consecuencia, se presentó un acceso restringido temporal a las plataformas Azure y Azure DevOps, desde el lunes 28 de julio a las 7:30 a. m hasta el martes 29 de julio a la 1:00 p. m.

Es importante aclarar que en ningún momento se afectó la disponibilidad de los servicios en producción ni se evidenció pérdida de información, el impacto se debió a la interrupción de los accesos a la plataforma administrativa del entorno de la suscripción *EAAlcaldiaMedellin*. Queremos resaltar que el acceso a dicho entorno fue recuperado mediante la creación de una nueva cuenta con el mismo nombre y su asignación como propietaria.

Durante el procedimiento de asignación de permisos de la cuenta Admindevops en el portal *EAAlcaldiaMedellin* se pudo evidenciar que la Subsecretaria Diana María Ochoa Henao contaba con un usuario con privilegios administrativos, con el cual era posible ingresar al portal de Azure y Azure DevOps en caso de requerirse.

A continuación, se presenta la respuesta frente a cada uno de los ítems solicitados en el oficio:

1. Explicación detallada del procedimiento técnico que llevó a la eliminación de la cuenta admindevops@medellin.gov.co.

R/= Ver Anexo 1: Informe de Incidente Portal Azure/Azure DevOps y Anexo 2: Correo “Problema UserPrincipalName en 365 o dominio” – TrackingID #2506120040012634.

2. Justificación del evento, incluyendo bitácora de actividades, responsables, trazabilidad y validaciones previas al procedimiento ejecutado.

   R/= Ver Anexo 3: Correo “Revisión seguimiento usuarios Directorio Activo y Office365”.

3. Copia del procedimiento formalizado que regula la eliminación de cuentas por parte del personal de la Mesa de Servicios.

   R/= La Mesa de Servicios opera bajo el marco de buenas prácticas ITIL; por tanto, la solicitud fue tratada como un requerimiento, conforme al proceso establecido de “Gestión de Requerimientos” (ver Anexo 4).

   Posteriormente, tras el incidente, se trabajó en conjunto con el equipo de Infraestructura en la formalización del procedimiento de “Gestión de Eliminación de Cuentas”, con el objetivo de asegurar una adecuada validación y control de la información relacionada. Este procedimiento se encuentra documentado en el Anexo 5: “Procedimiento Gestión de Eliminación de Cuentas”.

4. Protocolo o autorizaciones requeridas para que un especialista SAMI ejecute este tipo de acciones, y si fueron cumplidas en este caso.

   R/= Como se indicó previamente, estas acciones se enmarcan en el “Proceso de Gestión de Requerimientos” (ver Anexo 4), el cual establece los protocolos necesarios para su ejecución. En este caso específico, se cumplió con lo establecido, y la acción quedó registrada en la herramienta de gestión Aranda, bajo el requerimiento N.° 457584 (ver Anexo 6).

   Para la ejecución técnica, se siguió el procedimiento oficial de Microsoft para la creación o eliminación de usuarios en Microsoft Entra ID, disponible en el siguiente enlace: Procedimiento oficial de Microsoft Entra ID.

   Como acción de mejora, se ha incorporado el procedimiento específico denominado “Gestión de Eliminación de Cuentas”, con el objetivo de reforzar el control y la trazabilidad de este tipo de actividades (ver Anexo 5).

5. Indicar si se encuentran implementadas políticas de acceso condicional en Microsoft Entra, y si se trató de un proceso de eliminación de licencias, cierre de evaluación, cancelación de suscripciones o intervención sobre servicios de prueba.

R/= Actualmente se encuentran implementadas políticas de acceso condicional en Microsoft Entra. Ver Anexo 7: Instructivo “MFA – Autenticación multifactor”. Respecto a la trazabilidad del caso, se puede consultar el detalle en el Anexo 6.

6. Informar qué mecanismos de comunicación interna y control existen para evitar activaciones, eliminaciones o intervenciones no autorizadas.

   R/= Las solicitudes de eliminación de cuentas, tanto individuales como masivas, deben gestionarse a través de la herramienta Aranda y/o mediante correo electrónico, con previa autorización del área de TI Soporte. Ver Anexo 2, Anexo 3 y Anexo 6.

7. Entregar el flujo detallado de atención ante detección de inconsistencias en cuentas (como errores en el User Principal Name), con base en buenas prácticas de Microsoft, incluyendo etapas, responsables, tiempo de retención en la papelera y validación de permisos asociados.

   R/= Ver Anexo 4: Proceso Gestión de Requerimientos y Anexo 5: Procedimiento Gestión de Eliminación de Cuentas.

De manera adicional, se comparten las sesiones grabadas durante el procedimiento de recuperación entre las partes involucradas y de común acuerdo (Mesa de Servicios SAMI y Distrito de Medellín) el día 29 de julio identificadas de la siguiente manera:

- Revisión usuario AdminDevOps-20250729_111347-Grabación de la reunión
- Revisión usuario AdminDevOps-20250729_115845-Grabación de la reunión
- Revisión usuario AdminDevOps-20250729_133521-Grabación de la reunión 1

En estas se registran las actividades ejecutadas por parte de la Mesa de Servicios para el restablecimiento de la cuenta *admindevops@medellin.gov.co* eliminada de manera no intencional y posterior restauración de acceso a las plataformas Azure y Azure DevOps.

Toda la documentación antes mencionada, se encuentra disponible en la siguiente ruta del SharePoint: DM-TIGO-SAMI- 014-05082025.

Agradecemos la atención prestada y quedamos atentos a cualquier requerimiento adicional.

Cordialmente,



Brian Steve Bautista Guzmán
Supervisor de proyecto cliente
Direccion de Operaciones B2B
Vp de Negocio de Empresas y Gobierno