PROCEDIMIENTO		
Proceso - Subproceso: Gestión de TIC – Gestión de Seguridad de la Información	**Página: 1 de 8**	
Procedimiento: Revisión, actualización de cuentas y segregación de funciones. (Público)	**Código:** MPFT0212P	**Versión: 02**

Objetivo

Mantener ajustados los permisos de control de acceso a los aplicativos, desarrollar y mantener la segregación de privilegios en los controles de acceso para el uso de la información de la Empresa en los aplicativos de parte de cada uno de sus usuarios, manteniendo como principio la asignación del menor privilegio para el tratamiento de un activo de información.

Alcance.

Las direcciones a través de los Directivos de EAAB, son quiénes deben efectuar la revisión de los accesos y privilegios para que los usuarios puedan realizar sus funciones de trabajo mediante la utilización de activos de información y aplicativos de la EAAB-ESP.

A quienes diseñan los roles de accesos y privilegios para la utilización de los activos de información y aplicativos de la EAAB-ESP, requeridos para realizar las funciones de trabajo definidas en conjunto con los Dueños de las aplicaciones y servicios.

Una vez efectuada las revisiones de los roles de acceso y privilegios, si encontraron alguna novedad o actualización se culmina con realizar un registro a través de las herramientas definidas para ello.

Términos y definiciones.

ACTIVO OBJETIVO- AO:
Activo de información al que le aplica el control de acceso y el criterio de segregación. Encajan en este tipo de activos las aplicaciones / sistemas de información y los recursos de infraestructura informática que soportan los servicios de aplicaciones. Se denomina “AO” en este documento.

APROBADOR:
Se refiere al Directivo de la EAAB-ESP, en adelante *Aprobador*

ARCHER:
Se refiere a la herramienta de Gobierno, Riesgo y cumplimiento.

CONSULTOR DE CONTROL DE ACCESO:
Responsable de coordinar las actividades, de enviar a las áreas la “Matriz de Cuentas y Permisos”, y disposición para resolver dudas que le permitan actualizar y ajustar los permisos de acceso.

PREPARADOR:

Se refiere a la persona designada por el Directivo del área quien crea los formularios - SIMI, para las solicitudes de cuentas y permisos y registra su atención en la "Matriz de Cuentas y Permisos" del área.

SIMI:
Se refiere al sistema integrado manejo de identidades

USUARIO
Se refiere a toda persona natural o jurídica que accede a una aplicación de la empresa.

VALIDADOR:
Se refiere al funcionario delegado quien valida las solicitudes.

Normatividad

- Resolución 305 de 2008. Comisión Distrital de Sistemas (CDS) de Bogotá D.C
- Resolución 740 de 2018. "Por la cual se adopta la Política de Seguridad y Privacidad de la Información de la EAAB-ESP.
- Resolución 1236 de 2018. Por la cual se adopta la Política de tratamiento de Datos Personales para la EAAB-ESP.

Políticas Generales y de Operación.

1. MINIMA SEGREGACIÓN PARA CADA ACTIVO DE INFORMACIÓN

Para cada activo objetivo AO se debe realizar una segregación mínima de roles, que busca evitar que una misma persona tenga control sobre dos o más transacciones sensibles e incompatibles.

2. MINIMA SEGREGACIÓN PARA CADA RECURSO, APLICATIVO Y AMBIENTE CON CONTROL DE ACCESO

- El rol de Usuario debe estar segregado en cuanto a las actividades de cada proceso modelado en el aplicativo. Un mismo usuario no puede ostentar permisos para realizar actividades de Inicio, registro y resolución del trámite dentro del aplicativo. Es decir no podrá ser "juez y parte" dentro del aplicativo donde se gestiona el proceso.
- Si un aplicativo no tiene segregación debe tener controles compensatorios acordados con Seguridad de la información, TI y el área de negocio.

3. PRINCIPIO DE USO PARA CADA AMBIENTE (Desarrollo, Calidad y Producción) Y EL MODELO DE CAPAS DE UN APLICATIVO

- Los usuarios finales no deben tener acceso a los ambientes de desarrollo y Calidad si no existe una justificación expresa para su uso debidamente aprobado por el Directivo del área y "dueño" del aplicativo.
- El acceso a Productivo lo deben tener solamente los usuarios dispuestos por el Aprobador y "dueño" del aplicativo.
- Los administradores y responsables de la plataforma sólo pueden tener acceso al aplicativo durante un cambio autorizado expresamente y por tiempo limitado.
- El acceso a Desarrollo lo debe tener solamente el personal responsable de los desarrollos de los aplicativos de la Empresa.
- El acceso de Calidad lo debe tener solamente los roles que van a realizar pruebas de tipo funcional autorizados por el dueño del aplicativo.
- El acceso a cualquier ambiente lo autoriza y vigila el Aprobador.
- El acceso a las fuentes y cualquier cambio debe estar respaldado por un cambio controlado.

4. PRINCIPIOS DE SEGREGACIÓN

- Todo acceso a un AO debe contener los mínimos privilegios para el desarrollo de las funciones del usuario. con la función del usuario manteniendo como principio la asignación del menor privilegio para el tratamiento de un activo de información.
- Nadie debe tener todos los privilegios que le permitan iniciar y cerrar una misma operación en un proceso de negocio, es decir "ser juez y parte".
- Ninguna persona ajena al proceso de negocio debe disponer de acceso permanente con privilegios de cambios en ambiente productivo.
- Solo deben tener acceso permanente a la aplicación en ambiente productivo y la infraestructura las personas que soportan la operación.

5. PRINCIPIOS QUIEN PREPARA:

- Verificar la necesidad del área y propone las cuentas de acceso a los aplicativos para los funcionarios- usuarios.
- Identificar y reportar incidentes en los privilegios de uso de cada activo de información.
- Mantener actualizada la documentación de la "Matriz de Cuentas y Permisos" del área.
- Revisar la "Matriz de Cuentas y Permisos", reportando los riesgos, las desviaciones y los cambios necesarios, como plan de tratamiento, para mantener correcta la segregación de privilegios de acuerdo con las necesidades de negocio y las funciones establecidas por el Directivo del área.

- Informar al Aprobador de las desviaciones registradas en la “Matriz de Cuentas y Permisos” del área.
- Notificar las desviaciones en la herramienta GRC.

6. PRINCIPIOS QUIEN APRUEBA:

- Definir los accesos y privilegios requeridos en el control de acceso de sus funcionarios a una aplicación donde se gestionan los activos de información, de acuerdo con las necesidades del negocio, preservando la segregación de privilegios.
- Conocer, revisar, aprobar y mantener actualizada la “Matriz de Cuentas y Permisos” de su área de negocio.
- Tomar la iniciativa de revisar y pedir corte de la matriz cada vez que haya cambios de funciones y novedades de personal.

PROCEDIMIENTO		
Proceso - Subproceso: Gestión de TIC – Gestión de Seguridad de la Información	**Página: 5 de 8**	
Procedimiento: Revisión, actualización de cuentas y segregación de funciones. (Público)	**Código:** MPFT0212P	**Versión: 02**

ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE (DEPENDENCIA Y CARGO)	DOCUMENTOS Y REGISTROS
1. COORDINAR TAREAS			
1.1. Lanzar y coordinar la campaña con cada Dirección o Gerencia para el desarrollo/actualización de la Matriz de Cuentas y Permisos por cada activo de información del área. 1.2. Notifica por correo corporativo al Director de área el inicio de la actividad de revisión de los planes de remediación de segregación de cuentas y permisos.	Notificación por correo	Aprobador / Consultor de Control de Acceso	MPFT0212F01 Matriz de Cuentas y Permisos .
2. DESARROLLAR / ACTUALIZAR LA MATRIZ DE PERFILES Y PRIVILEGIOS			
2.1. Actualizar la matriz de revisión de Cuentas y permisos de cada área. 2.2. Identificar perfiles con conflicto, y/o no autorizados, y reportarlos por medio del procedimiento de manejo de incidentes en seguridad de la información que establece: El Usuario de la Información debe realizar las notificaciones al Centro de Servicio - CS / Dirección Servicios de Informática, a través de la línea 7777. **Como ejemplos de incidentes se tienen**: • Roles no actualizados • Accesos/permisos diferentes a los requeridos de acuerdo con la		Aprobador/ Validador	MPFT0212F01 Matriz de Cuentas y Permisos

función. • Usuarios configurados no están activos. • Usuarios asociados a perfiles no adecuados de acuerdo con su función. • Perfiles sin el control de cambios respectivo que los formalizan. 2.3. Aplica la segregación mínima establecida en las Políticas generales para cada perfil dentro de la segregación de cuentas y permisos del AO de la información. No olvidar la nota que establece que se debe segregar adicionalmente el perfil del usuario, en funciones de crear, actualizar y eliminar.			
3. IDENTIFICAR DESVIACIONES EN LA MATRIZ DE CUENTAS Y PERMISOS			
Cada perfil de usuario para cada activo de información debe ser verificado para identificar las desviaciones a que están expuestos, basados en los resultados de la revisión y en la experiencia del funcionario que realiza el análisis, de la matriz de cuentas y permisos. Si no se pueden segregar más los perfiles de los usuarios que no cumplen, debe realizar las actividades que permitan reducir el impacto y/o la probabilidad establecida en el análisis de riesgo actual –controles compensatorios.		Aprobador/ Validador	MPFT0212F01 Matriz de Cuentas y Permisos , con el registro SIMI de las desviaciones identificadas

La matriz resultante servirá le permitirá identificar cuántas actualizaciones tiene pendientes a la fecha y reportarlo en el indicador APA a la Dirección de Planeamiento y Control de Resultados que permitirá a la Empresa obtener un indicador del nivel de actualización de permisos informáticos corporativo.			
4. GESTIONAR FORMULARIOS SIMI PARA APLICAR CAMBIOS			
4.1. Gestión de los formularios SIMI	Formularios SIMI asignados y registrados en la matriz de cuentas y permisos.	Preparador/ Aprobador	Aplicativo SIMI
5. REVISAR / APROBAR MATRIZ DE CUENTAS Y PERMISOS			
5.1. Verificar cambios. 5.2. Aprueba / Rechaza lo correspondiente a los privilegios en el uso de cada activo de información de su área y es responsabilidad del Directivo donde declara la "prueba judicial" (No-repudio) 5.3. Reporta las desviaciones en la aplicación de Acuerdos de Gestión (APA) el indicador a la Dirección de Planeamiento y Control de Resultados Si la matriz de Cuentas y Permisos no es aprobada, retornar a la actividad.	Acuerdos de Gestión	Preparador /Aprobador	- Formularios SIMI procesados - Acuerdos de Gestión (APA)
6. COMUNICAR			

6.1. Notifica y reporta las desviaciones en la aplicación de Acuerdos de Gestión (APA) el indicador a la Dirección de Planeamiento y Control de Resultados 6.2. Mantener el registro de control con los cambios del día a día sobre la última matriz aprobada	-Indicador de Acuerdos de gestión.	Aprobador	Matriz de Cuentas y Permisos MPFT0212F01
7. MONITOREAR RIESGO			
7.1. Cualquier desviación no justificada será reportada y tratada como un incidente en seguridad de la información.		Áreas de negocio / 7777	Registro de incidentes en la herramienta GRC