1. OBJETIVO

Realizar, de manera sistemática y verificable, el monitoreo mensual de los roles y perfiles asignados a los usuarios que interactúan con los sistemas de información institucionales, y garantizar que los accesos otorgados estén debidamente justificados, actualizados y alineados con las funciones y responsabilidades del usuario, conforme al principio de menor privilegio definido por el SGSPI (Sistema de Gestión de Seguridad y Privacidad de la Información) y a lo dispuesto en el Manual de políticas y lineamientos de seguridad de la Información MN-IIT-0072.

2. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Procedimiento	PR-IIT-0455	Gestión de accesos	Digital	Interno
Instructivo	IN-IIT-0273	Operaciones para la gestión de accesos	Digital	Interno
Instructivo	IN-IIT-0105	Modificación del Anexo “Roles de las soluciones tecnológicas”	Digital	Interno
Manual	MN-IIT-0072	Manual de políticas y lineamientos de seguridad de la información	Digital	Interno
Anexo	Anexo	MN-IIT-0072 Definiciones y siglas de seguridad y privacidad	Digital	Interno

3. DEFINICIONES Y SIGLAS

Todas las definiciones y siglas presentadas en el contenido de este documento están exhaustivamente detalladas y explicadas en el Anexo MN-IIT-0072 Definiciones y Siglas de Seguridad y Privacidad de la Información, el cual ha sido cuidadosamente elaborado para proporcionar una comprensión precisa y completa de los conceptos utilizados.

4. DESARROLLO DEL TEMA

4.1 Lineamientos generales

El monitoreo mensual de roles y perfiles tiene como finalidad detectar oportunamente:

- Inconsistencias.
- Accesos innecesarios.
- Cuentas inactivas o privilegios no justificados.

La OSI es la encargada de coordinar y consolidar el proceso, pero la responsabilidad de verificar y validar los accesos corresponde a los jefes inmediatos, responsables de área y administradores de sistemas, garantizando un enfoque de corresponsabilidad.

En este marco, la OSI deberá mantener mecanismos de auditoría interna trimestral orientados a fortalecer la mejora continua del proceso, así como un historial consolidado y firmado digitalmente que respalde cada ciclo mensual de revisión. La documentación y los hallazgos deberán conservarse en repositorios seguros con control de versiones, lo cual permitirá la trazabilidad y la evaluación continua del cumplimiento

4.2 Paso a paso del proceso de monitoreo mensual

I. Recolección de reportes de usuarios y roles activos
El responsable de cada sistema debe recolectar mensualmente el reporte de usuarios y roles activos, que incluya la identificación del usuario, dependencia, cargo, nombre del sistema, fecha de último acceso y privilegios asignados. Esta información se consolida y se remite a la OSI antes del día 3 hábil de cada mes.

II. Cruce con planta y novedades de Talento Humano
La OSI compara los datos recopilados con la planta de personal vigente y las novedades administrativas (retiros, licencias, comisiones, etc.), asegurando que los accesos correspondan a personal activo y a sus funciones actuales.

III. Análisis técnico y aplicación de filtros
La OSI o el área de Soporte Técnico aplica filtros técnicos (manuales o automatizados) para identificar:
a. Privilegios elevados sin justificación.
b. Accesos inactivos o innecesarios.
c. Combinaciones riesgosas o duplicadas de roles.

IV. Clasificación de hallazgos
Los hallazgos se clasifican según su criticidad:
a. Crítico: acceso indebido a información sensible.
b. Medio: incompatibilidades o conflictos de rol.
c. Leve: asignaciones innecesarias.

V. Validación de hallazgos con jefes de área
La OSI remite los hallazgos a los jefes de área responsables para su validación y la justificación o solicitud de eliminación de accesos no pertinentes.

VI. Aplicación de ajustes autorizados
El equipo de Soporte Técnico realiza los ajustes solicitados y autorizados en los sistemas, generando tickets de cambio que documentan las acciones realizadas con trazabilidad completa.

VII. Registro de evidencias
La OSI registra y archiva toda la evidencia generada: tickets cerrados, capturas de pantalla, formatos firmados y validaciones documentadas, consolidándolas en un repositorio seguro con control de versiones.

VIII. Generación del informe mensual
La OSI elabora y valida un informe mensual que consolida los hallazgos, las acciones correctivas aplicadas, los indicadores clave y las recomendaciones para fortalecer el control de accesos.

IX. Archivo y seguimiento
El informe final y sus soportes se archivan en un repositorio digital seguro y controlado. Los hallazgos críticos se presentan en el Comité de Seguridad y se da seguimiento a las acciones de mejora continua, consolidando así la mejora permanente del proceso.

5. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	24/06/2025		Versión Inicial	Esta versión corresponde a Información Pública

Elaboró:	Alvaro Antonio Sarria Romero, Felipe Alberto Portocarrero Ramirez. **Elaboración técnica**	Gestor IV Gestor III	Oficina de Seguridad de la Información
	Tito Alejandro Menjura Murcia, César Augusto Garzón Baquero **Elaboración metodológica**	Gestor II Gestor I	Coordinación de Procesos y Riesgos Operacionales - Subdirección de Procesos.
Revisó:	Andrés Ricardo Castelblanco Mendoza	Subdirector	Subdirección de Infraestructura Tecnológica y de Operaciones

	Francisco Andrés Daza Cardona	Jefe	Oficina de Seguridad de la Información
Aprobó:	Andrés Ricardo Castelblanco Mendoza	Subdirector	Subdirección de Infraestructura Tecnológica y de Operaciones
	Francisco Andrés Daza Cardona	Jefe	Oficina de Seguridad de la Información