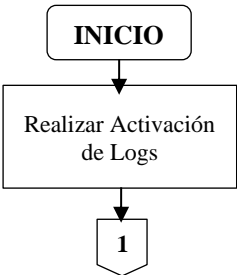


	GESTIÓN DE TICS	CÓDIGO	E-GTIC-PR-008
		VERSIÓN	02
	GESTIÓN DE LOGS DE EVENTOS Y TRAZABILIDAD DE LAS OPERACIONES	PÁGINA	1 de 3
		VIGENTE DESDE	04/10/2022

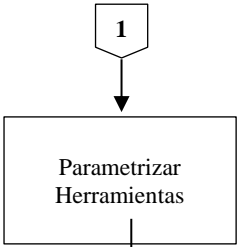
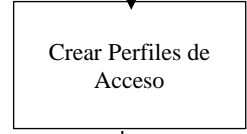

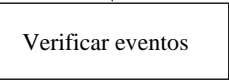
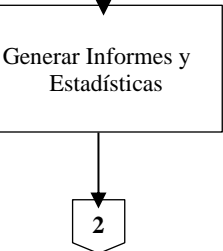
1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO	
OBJETIVO	Establecer las actividades que deben ejecutarse para registrar, revisar y conservar los registros las actividades de los usuarios, las fallas o las transacciones en los sistemas de información, bases de datos y sistemas operativos de los servicios tecnológicos con la finalidad de tomar acciones oportunas y garantizar la seguridad y privacidad de las transacciones y operaciones en los activos de Información del Instituto.
ALCANCE	Inicia con la Activación de los logs en las diferentes plataformas tecnológicas que posee la Entidad y finaliza la generación de informes para la adecuada toma de decisiones sobre la operación idónea de cada una de ellas.

2. GLOSARIO	
Término	Definición
ADMINISTRACIÓN DE LOG	Seguimiento, monitoreo y generación de reportes a Log de eventos y trazabilidad en las plataformas tecnológicas con la finalidad de tomar acciones de mejora y controles frente a incidentes y continuidad de las operaciones.
EVENTOS	Son acciones relacionadas con una alerta o notificación detectada por aplicaciones informáticas.
INCIDENTE	Son eventos no programados o no deseados que comprometen la integridad, confidencialidad o disponibilidad de las aplicaciones o los datos lo cual puede comprometer la operación normal de la Entidad o convertirse en una amenaza.
LOG	Son registros de eventos que ocurren en las plataformas informáticas y están relacionadas con el acceso a sistemas operativos, sistemas de información, conectividad, acceso a redes, aplicaciones o eventos de seguridad.
PLATAFORMAS TECNOLÓGICAS	Son elementos de Software o Hardware que permiten ejecutar y realizar tareas con fines específicos como son los sistemas de información, bases de datos, sistemas operativos de los servicios tecnológicos, elementos de seguridad y conectividad de red, etc.
TRAZABILIDAD DE TRANSACCIONES	Es el seguimiento, monitoreo y procedimientos que permiten identificar y registrar eventos ocurridos en las plataformas tecnológicas existentes.
PLAN DE RESPALDO	Procedimiento que permite determinar y ejecutar de manera organizada actividades para la recuperación ante fallas o incidentes teniendo en cuenta el manejo y administración de copias de respaldo, procesos y plataformas de restauración.

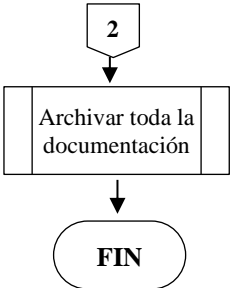
3. CONDICIONES GENERALES	
No.	Descripción
1	Se debe contar con herramientas y configuración de los logs presentes en las diferentes plataformas tecnológicas de acuerdo a su naturaleza o diseño para poder registrar y hacer seguimiento de las actividades de los usuarios, fallas o eventos de seguridad que puedan presentarse, como son en los servidores, sistemas de información o aplicaciones, sistemas operativos, soluciones de monitoreo de red y seguridad.
2	Se debe definir el esquema y almacenamiento de los log para su custodia y análisis además para manejo de incidentes en caso de ser necesario.
3	Seleccionar y definir cuidadosamente las transacciones a las que se le deba hacer seguimiento como son identificadores de usuarios, accesos exitosos o rechazados, fechas, horas, detalles de eventos claves, eventos con acceso de usuarios que poseen privilegios especiales.
4	Aplicar los controles necesarios de acuerdo al Modelo de Seguridad y Privacidad de la información en especial a lo estipulado en los controles del Numeral 12.4 Registro y Seguimiento de la NTC- ISO/IEC 27001.
5	Cuando el servicio dependa de un tercero (<i>Proveedor – Soporte de tercer nivel</i>), se deberá tener en cuenta e incluir dentro de las obligaciones contractuales las acciones de seguimiento y monitoreo de eventos (como son: actividades de configuración de herramientas, activación, verificación seguimiento de logs y generación de informes y evidencias necesarias) lo cual se realizará en coordinación con el supervisor del contrato.

4. DESARROLLO DEL PROCEDIMIENTO						
No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
1		Realizar la activación de registros de logs y auditorías en las plataformas tecnológicas que posee la Entidad. (módulos o tablas).	Profesionales y Técnicos Oficina de Tecnologías de la Información y las Comunicaciones			Max: 90 Minutos Min: 30 minutos Prom:60 minutos

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-PR-008
		VERSIÓN	02
	GESTIÓN DE LOGS DE EVENTOS Y TRAZABILIDAD DE LAS OPERACIONES	PÁGINA	2 de 3
		VIGENTE DESDE	04/10/2022

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
2		Configurar la herramienta propia de la consola de la plataforma tecnológica de acuerdo a la operación de la Entidad. Nota: Se deberá tener en cuenta el inventario de aplicaciones que posee la Entidad y parametrizar cada una de las características que posee la herramienta.	Profesionales y Técnicos Oficina de Tecnologías de la Información y las Comunicaciones			Max: 180 minutos Min: 30 minutos Prom: 105 minutos
3		Crear los perfiles de acceso a las diferentes plataformas, de acuerdo con Roles y permisos definidos por la Oficina de Tecnologías de la Información y las Comunicaciones o requeridos en la Entidad. Nota: Se deberá tener en cuenta la definición de roles de la Oficina de Tecnologías de la Información y las Comunicaciones	Profesionales y Técnicos Oficina de Tecnologías de la Información y las Comunicaciones		Formato: Gestión de Usuarios E-GTIC-FT-014	Max: 60 minutos Min: 30 minutos Prom: 45 minutos
4		Elaborar planes de respaldo para el manejo de eventos en las plataformas de servicios tecnológicos. Elaborar Planes de restauración (imágenes, copia de respaldo y reporte de incidentes)	Profesionales y Técnicos Oficina de Tecnologías de la Información y las Comunicaciones		Formato: Bitácora de backup de información E-GTIC-FT-011	Max: 210 minutos Min: 60 minutos Prom: 130.5 minutos
5		Realizar seguimiento de errores, eventos y trazabilidad. El administrador de la plataforma debe revisar en el módulo o herramienta del sistema los eventos generados.	Profesionales y Técnicos Oficina de Tecnologías de la Información y las Comunicaciones	X	Formato: Registro de eventos y trazabilidad de sistemas de información Formato: Registro de eventos y trazabilidad de plataformas tecnológica	Max: 210 minutos Min: 30 minutos Prom: 120 minutos
6		Generar informes y estadísticas sobre los eventos y trazabilidad encontrados en las plataformas.	Profesionales y Técnicos Oficina de Tecnologías de la Información y las Comunicaciones		Formato: Registro de eventos y trazabilidad de sistemas de información Formato: Registro de eventos y trazabilidad de plataformas tecnológica	Max: 90 minutos Min: 30 minutos Prom: 60 minutos

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-PR-008
		VERSIÓN	02
	GESTIÓN DE LOGS DE EVENTOS Y TRAZABILIDAD DE LAS OPERACIONES	PÁGINA	3 de 3
		VIGENTE DESDE	04/10/2022

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
7		Archivar toda la documentación generada a lo largo del procedimiento según el instructivo de gestión documental.	Profesional, Técnico o Auxiliar de la Oficina de Tecnologías de la Información y las Comunicaciones		Instructivo: Organización archivo de gestión A-GDO-IN-001	Max: 60 minutos Min: 30 minutos Prom: 45 minutos

5. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Creación del documento Se realiza la creación de documento para contar con mecanismos que aseguren el registro y trazabilidad de las Operaciones en las plataformas tecnológicas de la Entidad.	03/11/2021	ORALIA FRANCO GÓEZ PROFESIONAL – CONTRATISTA Área de Sistemas VERONICA BORGES CELIN TÉCNICO Área de Sistemas
02	1. Se realiza la actualización de las áreas / dependencias y cargos mencionados en el documento con el fin de dar cumplimiento a lo establecido en el Acuerdo “Por el cual se modifica la Estructura Organizacional del INSTITUTO DISTRITAL PARA LA PROTECCIÓN DE LA NIÑEZ Y LA JUVENTUD IDIPRON, se establecen las funciones de sus dependencias y se dictan otras disposiciones” 2. Se realiza el ajuste de la codificación de los formatos y documentos mencionados en el procedimiento (manual, documento interno o instructivo), de acuerdo con los ajustes realizados a los códigos de los documentos del Sistema Integrado de Gestión producto del rediseño institucional. 3. Se realiza cambio de código del documento del A-TIC-PR-008 al código E-GTIC-PR-008	04/10/2022	MARISOL MONSALVE USME PROFESIONAL OFICINA ASESORA DE PLANEACIÓN

6. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	VIVIANA ANDREA SANCHEZ MORALES	PROFESIONAL OFICINA ASESORA DE PLANEACIÓN	04/10/2022
APROBACIÓN LÍDER DE PROCESO	FABIAN ANDRÉS CORREA ÁLVAREZ	JEFE OFICINA ASESORA DE PLANEACIÓN	04/10/2022