

### CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	15/12/2023	Nuevo procedimiento.

### OBJETIVO

Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisfice todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.

### ALCANCE

Inicia con identificar, documentar y supervisa las actividades de control, se continua asignar roles, responsabilidad y asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, finaliza con revisar y definir errores de proceso de información y aplicar las políticas de clasificación de datos y uso aceptable y seguridad, los procedimientos para proteger los activos de información bajo el control del negocio.

### DEFINICIONES Y SIGLAS

Siglas:

1. TI: Tecnologías de la Información.
2. OTIC: Oficina de Tecnologías de la información y las comunicaciones.

### POLÍTICAS DE OPERACIÓN Y ASPECTOS GENERALES

1. Las actividades que son punto de control, serán señaladas dentro del Flujoograma con la figura de cuadrado y la sigla punto de control (P.C.) dentro de ella.
2. Cuando en las actividades se presenten incumplimiento de requisitos de norma o de los clientes y/o usuarios, deberán implementarse el procedimiento denominado "Acciones correctivas, preventivas y de mejora".
3. Cuando dentro del procedimiento se incluyan acciones de divulgación o comunicación estas deberán realizarse en el marco del Plan de comunicaciones del Departamento y deberá tener en cuenta los procedimientos y protocolos establecidos.

### PRODUCTO O SERVICIO

SALIDAS (Producto o Servicio)	DESCRIPCIÓN	GRUPOS DE VALOR OBJETIVO
<ol style="list-style-type: none"> <li>1. Resultados de las revisiones de la efectividad de procedimiento.</li> <li>2. Recomendaciones y análisis de las causas raíces.</li> <li>3. Informe de violaciones de seguridad de la información.</li> </ol>	1. Mantener la integridad de la información y la seguridad de los activos de información manejados dentro de los procesos comerciales en la empresa o tercerizados.	Usuarios internos

### NORMATIVIDAD Y/O DOCUMENTOS ASOCIADOS

- El control de los riesgos a la seguridad de la información, riesgos laborales, aspectos ambientales se pueden consultar el Mapa de Riesgos.
- La normativa asociada al procedimiento se puede consultar en la Matriz de requisitos legales y normativos
- Los documentos asociados al procedimiento se pueden consultar en el Listado Maestro de Documentos.
- Los registros asociados al procedimiento se pueden consultar en el Listado Maestro de registros/ Cuadro de Caracterización Documental
- Las disposiciones de almacenamiento y archivo se pueden consultar en las Tablas de Retención Documental.

ACTIVIDAD	FLUJOGRAMA	DESCRIPCIÓN ACTIVIDAD	TIEMPO	RESPONSABLE	FORMATO Y/O REGISTRO
		INICIO.			
1		Identificar y documentar las actividades de control de los procesos de negocio claves para satisfacer los requerimientos de control para los objetivos estratégicos, operacionales, de informes y cumplimiento.	Anual	Servidor asignado de la seguridad de la información de la Entidad.	
2		Supervisar continuamente las actividades de control de extremo a extremo para identificar oportunidades de mejora.	Anual	Servidor asignado de la seguridad de la información de la Entidad.	<a href="#">Plan de mejora continua</a>
3		Crear transacciones por individuos autorizados siguiendo los procedimientos establecidos, incluyendo, cuando sea apropiado, la adecuada segregación de tareas en relación al origen y aprobación de esas transacciones.	Cuando se requiera	Mesa de servicios	<a href="#">127-FORGI-09 FORMATO ÚNICO DE SISTEMAS</a>
4		Asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocio asignadas.	Cuando se requiera	Mesa de servicios	
5		Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, basados en los roles de puesto predefinidos. Eliminar o revisar los derechos de acceso inmediatamente si el rol del puesto cambia o un miembro del personal deja el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso es adecuado para las actuales amenazas, riesgos, tecnología y necesidades del negocio.	Cuando se requiera	Mesa de servicios	




6	<a href="#">Anexo 1- Flujoograma</a>	Revisar periódicamente las definiciones de control de acceso, registros e informes de excepciones para asegurar que todos los privilegios de acceso son válidos y están alineados con el personal actual y sus roles asignados.	Cuando se requiera	Mesa de servicios	
7		Definir y mantener procedimientos para asignar propiedad, corregir errores, reemplazar errores y manejar las condiciones fuera de equilibrio.	Anual	Servidor asignado de la seguridad de la información de la Entidad.	
8		Hacer seguimiento, corregir, aprobar y reenviar documentos fuente y transacciones.	Semestral	Servidor asignado de la seguridad de la información de la Entidad.	<a href="#">Formato registro, actualización y valoración de Activos de Información</a>
9		Revisar e Informar acerca de errores de proceso de información relevantes de manera oportuna para realizar el análisis de tendencias y causas raíces.	Cuando se requiera	Servidor asignado de la seguridad de la información de la Entidad.	<a href="#">Formato registro, actualización y valoración de Activos de Información</a>
10		Definir requerimientos de retención, basados en los requerimientos de negocio, para conocer las necesidades operativas, de reporte financiero y cumplimiento.	Anual	Servidor asignado de la seguridad de la información de la Entidad.	
11		Capturar y eliminar la fuente de información, evidencia que la soporta y el registro de las transacciones, la evidencia que la soporta y el registro de transacciones de acuerdo con la política de retención.	Cuando se requiera	Servidor asignado de la seguridad de la información de la Entidad.	
12		Aplicar las políticas de clasificación de datos y uso aceptable y seguridad, los procedimientos para proteger los activos de información bajo el control del negocio, proporcionando concienciación y formación de un uso aceptable, Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación e Identificar e implementar procesos, herramientas y técnicas para verificar razonablemente el cumplimiento.	Anual	Servidor asignado de la seguridad de la información de la Entidad.	
13		FIN			

**AUTORIZACIÓN**

**ELABORÓ:**

**Leydi Tamara Rodriguez**  
Contratistas OTIC

**REVISÓ:**

  
**Carlos de la Ossa Hurtado**  
Jefe de la OTIC.

**APROBÓ:**

  
**Carlos de la Ossa Hurtado.**  
Jefe de la OTIC.



DIAGRAMA DE FLUJO  
PROCESO: GESTIÓN DE LA TECNOLOGÍA Y LA INFORMACIÓN  
PROCEDIMIENTO: GESTIONAR CONTROLES DE PROCESO DE NEGOCIO

