



# **PERSONERÍA DE BOGOTÁ, D. C.**

## **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 03 – PL – 06**

Direccionamiento TIC

Versión – 03  
27-01- 2023

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 03	<b>Página:</b> 2 de 13
		<b>Vigente desde:</b> 27/01/2023	

<b>CONTROL DE CAMBIOS</b>		
<b>VERSIÓN</b>	<b>FECHA</b>	<b>DESCRIPCIÓN DE LA MODIFICACIÓN</b>
1	29/01/2021	Versión inicial del documento
2	20/01/2022	Versión actualizada del documento
3	27/01/2023	Actualización cronograma de actividades

<b>Elaboró:</b>	<b>Revisó:</b>	<b>Aprobó:</b>
<b>Edgar Martín Cubides Rojas</b> Director de Tecnologías de la Información y las Comunicaciones – DTIC	<b>Héctor Hernán González Naranjo</b> Director Oficina de Planeación	Comité Institucional de Gestión y Desempeño

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 03	<b>Página:</b> 3 de 13
		<b>Vigente desde:</b> 27/01/2023	

## TABLA DE CONTENIDO

1. INTRODUCCIÓN .....	4
2. OBJETIVO GENERAL .....	4
3. ALCANCE .....	4
4. RESPONSABLES .....	5
5. DEFINICIONES.....	5
6. DESARROLLO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....	7
6.1 Principios de seguridad que soportan el Plan de Seguridad de la Información de la Personería de Bogotá D.C. ....	7
6.2 Descripción del Plan de Implementación del SGSI .....	8
6.3 Recursos y Presupuesto.....	10
7. NORMATIVIDAD APLICABLE .....	10
8. CRONOGRAMA.....	11

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 03	<b>Página:</b> 4 de 13
		<b>Vigente desde:</b> 27/01/2023	

## 1. INTRODUCCIÓN

Considerando que la seguridad de la información es un modelo de mejora continua enfocado a la protección de los activos de información y TI en términos de la preservación de la confidencialidad, integridad y disponibilidad de la información y las tecnologías de la información, con base en un enfoque de cumplimiento normativo, buscando el logro de los objetivos institucionales, la Personería de Bogotá, D.C. ha implementado y opera el Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma técnica ISO/IEC 27001:2013 y considerando lo dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC en cuando a la política de gobierno digital, el Modelo de Seguridad y Privacidad de la Información – MSPI, así como el Modelo Integrado de Planeación y Gestión, como conjunto de buenas prácticas en seguridad de la información, ciberseguridad y privacidad en las entidades del Estado colombiano.

El presente documento presenta las actividades y línea de tiempo a seguir por la Personería de Bogotá, D.C. respecto a las actividades de implementación, operación, fortalecimiento y mejora del Sistema de Gestión de la Seguridad de la información (SGSI) en todos los procesos de la entidad durante la vigencia 2023, siguiendo los lineamientos establecidos en la Norma NTC-ISO-IEC-27001 y las actividades descritas en el Modelo de Seguridad y Privacidad de la Información – MSPI de la Política de Gobierno Digital de MINTIC.

## 2. OBJETIVO GENERAL

Describir y programar las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información – MSPI, emitido por el Ministerio de Tecnologías de la Información y la Comunicaciones MINTIC en la Política de Gobierno Digital, y que se ejecutarán en el transcurso de la vigencia 2023, las cuales están alineadas con el marco normativo de la norma ISO 27001:2013 y la Política de Gobierno Digital.

## 3. ALCANCE

Programación y descripción de las actividades a realizar por la Personería de Bogotá, D.C. durante la vigencia 2023 sobre la implementación, operación, fortalecimiento y mejora del Sistema de Gestión de la Seguridad de la información (SGSI), de acuerdo con el Modelo de Seguridad y Privacidad de la Información - MSPI emitido por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, y la Norma técnica ISO/IEC 27001:2013.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

PERSONERÍA DE BOGOTÁ, D. C	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 03-PL-06	
		Versión: 03	Página: 5 de 13
		Vigente desde: 27/01/2023	

#### 4. RESPONSABLES

El Sistema de Gestión de la Seguridad de la Información (SGSI) es responsabilidad de la Dirección de Tecnologías de la Información y las Comunicaciones DTIC de acuerdo con lo establecido en la Resolución 406 de 2020, Artículo 22, donde se adopta el Modelo Integrado de Planeación y Gestión MIPG.

La alta dirección de la Personería de Bogotá D.C., incluyendo los Directores, Subdirectores, Jefes de oficina, Personeros delegados y locales, apoyarán la ejecución del presente plan mediante la participación y compromiso con las actividades que requieran de su apoyo y gestión y para las cuales se encuentra relacionado entre los responsables en la descripción del presente plan. Igualmente fomentará en el personal a cargo la participación en las actividades relacionadas con dicho plan.

#### 5. DEFINICIONES

**BCP:** Plan de Continuidad del Negocio (en inglés *Business Continuity Plan*), es un plan que define las actividades a realizar para que las organizaciones mantengan, restauren y recuperen sus actividades y funciones en un tiempo determinado, ante la ocurrencia de un evento o interrupción o deseada o programada que afecte sus operaciones.

**DRP:** Plan de Recuperación de Desastres (en inglés *Disaster Recovery Plan*) que describe las actividades del proceso de recuperación para que las organizaciones comiencen de nuevo sus actividades, ante la ocurrencia de un desastre que afecte sus operaciones.

**Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

**Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 03	<b>Página:</b> 6 de 13
		<b>Vigente desde:</b> 27/01/2023	

**IPV6:** Protocolo de internet versión 6. Es una versión del protocolo de internet IP, diseñada para reemplazar el protocolo IPV4.

**Mejor práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad en la entidad.

**MSPI:** Modelo de Seguridad y Privacidad de la Información. Herramienta diseñada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia - **MINTIC** para guiar la implementación del Sistema de Gestión de Seguridad SGSI.

**NORMA ISO 27001:** es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

**Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico

**Procedimiento:** Definen como las políticas, referencias técnicas, mejores prácticas y guías serán implementadas en una situación dada. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca cómo les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

**SGSI:** Sistema de Gestión de la Seguridad de la Información. Por sus siglas en inglés (*information security management system, ISMS*) es modelo de mejora continua enfocado a la protección de los activos de información y TI en términos de la preservación de la confidencialidad, integridad y disponibilidad de la información y las tecnologías de la información, con base en un enfoque de cumplimiento normativo, buscando el logro de los objetivos institucionales.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 03	<b>Página:</b> 7 de 13
		<b>Vigente desde:</b> 27/01/2023	

## **6. DESARROLLO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

### **6.1 Principios de seguridad que soportan el Plan de Seguridad de la Información de la Personería de Bogotá D.C.**

- La Personería de Bogotá D.C. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requisitos jurídicos aplicables de acuerdo con su naturaleza, así como los de carácter técnico, en especial ISO/IEC 27001:2013.
- La Personería de Bogotá, D.C. tiene el compromiso de proteger la información a lo largo de su ciclo de vida en cada una de las actividades definidas en sus procesos, así como su infraestructura tecnológica, de las amenazas aplicables.
- La Personería de Bogotá D.C. protegerá la información creada, obtenida, procesada, transmitida o almacenada por sus procesos de negocio, con el fin de minimizar impactos económicos, operativos, reputacionales y/o de cumplimiento por fallas en su gestión y uso. Para ello es esencial la aplicación de controles de acuerdo con los riesgos identificados y la clasificación de los activos de información.
- La Personería de Bogotá, D.C., protege la información a lo largo de su ciclo de vida con el fin de minimizar impactos económicos, reputacionales, operativos o de cumplimiento, así como sobre las personas debido a un uso incorrecto o no idóneo de esta mediante la aplicación de controles según el riesgo y criticidad del activo.
- La Personería de Bogotá, D.C., protege su información y tecnologías de las amenazas originadas por parte del personal y de forma externa.
- La Personería de Bogotá, D.C., protege las instalaciones de procesamiento y almacenamiento de información incluyendo la infraestructura tecnológica que soporta sus procesos críticos y de apoyo.
- La Personería de Bogotá, D.C., controla sus procesos de negocio garantizando la seguridad de los recursos tecnológicos, incluyendo hardware y redes de datos.
- La Personería de Bogotá, D.C., implementa el control de acceso a la información, incluyendo repositorios documentales, sistemas y servicios, así como los recursos de red, hardware y demás sistemas de apoyo, de la información en soporte físico y digital.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 03	<b>Página:</b> 8 de 13
		<b>Vigente desde:</b> 27/01/2023	

- La Personería de Bogotá, D.C., realiza una adecuada y oportuna gestión de eventos e incidentes de seguridad de la información, ciberseguridad y privacidad, y las debilidades o vulnerabilidades identificadas en los sistemas de información, asegurando una mejora efectiva de su modelo de seguridad.
- La Personería de Bogotá, D.C., implementa la seguridad como parte integral del ciclo de vida de los sistemas y servicios de información, y la documentación.
- La Personería de Bogotá, D.C., garantiza la disponibilidad de sus procesos de negocio y la continuidad de su operación, acorde a los impactos que pueden generar los eventos o incidentes disruptivos que puedan afectarlos.
- La Personería de Bogotá, D.C., exigirá el cumplimiento de las obligaciones legales, regulatorias, reglamentarias y contractuales establecidas en las políticas de seguridad y privacidad de la información, así como de carácter técnico.

## 6.2 Descripción del Plan de Implementación del SGSI

Las siguientes son las actividades para desarrollar en la vigencia 2023 para alcanzar el objetivo de seguridad en alineación con el MSPI de la Estrategia de Gobierno Digital y los requisitos de la norma ISO/IEC 27001:2013.

FASE DEL MSPI	META	ACTIVIDAD	RESPONSABLE
<b>PLANIFICACIÓN</b>	Gestión de activos de información.	Revisar y actualizar el inventario de activos de información - así como su clasificación - de los 16 procesos de la entidad en la matriz de activos de información.	Dirección DTIC, Líderes y demás responsables de los activos para cada uno de los procesos.
	Gestión de requisitos	Revisar y actualizar la matriz de los requisitos de orden jurídico (legales, regulatorios y reglamentarios) junto a los de tipo organizacional, técnico y contractual, incluyendo las partes interesadas de donde éstos surgen.	Dirección DTIC, Líderes y demás responsables de los procesos.
	Identificación, Valoración y tratamiento de riesgo.	Revisar y actualizar la metodología de gestión de riesgos de seguridad de la información, así como la matriz de riesgos, en cuanto a los riesgos identificados y su valoración, junto a la revisión de eficacia de controles establecidos alineado al Anexo A.	Dirección DTIC, Líderes y demás responsables de la gestión de riesgos de todos los procesos

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.



<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 03	<b>Página:</b> 9 de 13
		<b>Vigente desde:</b> 27/01/2023	

<b>FASE DEL MSPI</b>	<b>META</b>	<b>ACTIVIDAD</b>	<b>RESPONSABLE</b>
	Políticas de seguridad y privacidad de la información	Actualizar el manual con las políticas y lineamientos para la seguridad y privacidad de información, gestionar su aprobación y socializarlas.	Dirección de TIC, Dirección de Planeación y Comité Institucional de Gestión y Desempeño
	Procedimientos de seguridad de la información.	Revisar y actualizar procedimientos de seguridad de la información, así como generar los adicionales que sean necesarios (siempre que sean estos críticos para la organización), gestionar la aprobación y realizar su divulgación.	Dirección TIC, Dirección de Planeación y Comité Institucional de Gestión y Desempeño
	Plan de Comunicaciones	Revisar el plan de comunicación, sensibilización y capacitación SGSI.	Dirección de TIC Comité Institucional de Gestión y Desempeño
	Gestión de incidentes	Revisar y actualizar las metodologías y herramientas de gestión de eventos e incidentes con base en su eficacia.	Dirección de TIC
<b>IMPLEMENTACIÓN</b>	Implementación plan tratamiento de riesgos	Realizar seguimiento a la aplicación oportuna (periódica o por evento) de los controles establecidos en el plan de tratamiento de riesgos. Presentar los informes periódicos de seguimiento de riesgos de seguridad de la información incluyendo datos sobre la eficacia de los controles.	Oficina de Control interno
	Desarrollo y fortalecimiento de competencias y toma conciencia	Realizar una evaluación continua de las competencias en gestión segura de la información para cada una de las funciones y roles en la entidad. Mantener actualizado el programa de desarrollo y fortalecimiento de las competencias técnicas y de gestión (capacitación) y toma de conciencia, junto a la evaluación de su eficacia.	Dirección de TIC, Dirección de Planeación, Comité Institucional de Gestión y Desempeño y Dirección de Talento Humano
<b>EVALUACIÓN DE DESEMPEÑO</b>	Indicadores de Gestión	Realizar la medición y análisis de datos en los indicadores de gestión de seguridad de la información.	Dirección de TIC
	Plan de revisión y seguimiento, a la implementación del SGSI	Proyectar y aprobar el documento con el Plan de seguimiento y revisión del SGSI	Dirección de TIC, Dirección de Planeación y Comité Institucional de Gestión y Desempeño

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 03	<b>Página:</b> 10 de 13
		<b>Vigente desde:</b> 27/01/2023	

<b>FASE DEL MSPI</b>	<b>META</b>	<b>ACTIVIDAD</b>	<b>RESPONSABLE</b>
	Plan de Ejecución de Auditorías	Ejecución de auditorías programadas (interna) al Sistema de Gestión de la Seguridad de la Información (SGSI) según el programa de auditoría.	Oficina de Control interno
	Revisión por la dirección	Realizar la revisión por la dirección al SGSI asegurando la incorporación de las entradas y salidas definidas en la norma ISO/IEC 27001.	Dirección de TIC

### **6.3 Recursos y Presupuesto**

El desarrollo del presente plan podrá ser realizado con personal externo como contratistas o servicios de consultoría, o con el personal de planta según las funciones y obligaciones de los respectivos cargos y procesos de la entidad. El presupuesto para la implementación del Plan de Seguridad y Privacidad de la Información de la Personería de Bogotá D.C., está incluido dentro del rubro asignado a cada una de las dependencias responsables de las actividades programadas para la vigencia 2023.

### **7. NORMATIVIDAD APLICABLE**

<b>TIPO DE NORMA</b>	<b>NÚMERO</b>	<b>AÑO</b>	<b>EMISOR</b>	<b>ARTÍCULOS (APLICACIÓN)</b>
Norma técnica ISO	31000	2018	ISO	Proceso de gestión de riesgo
Norma técnica ISO/IEC	27005	2018	ISO	Proceso de gestión de riesgo
Norma técnica ISO/IEC	27001	2013	ISO	Toda la norma.
Norma técnica ISO/IEC	27032	2012	ISO	Proceso de gestión de riesgo Controles Gestión de activos

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

PERSONERÍA DE BOGOTÁ, D. C	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 03-PL-06	
		Versión: 02	Página: 11 de 13
		Vigente desde: 20/01/2022	

## 8. CRONOGRAMA

No.	ACTIVIDAD	INDICADOR	2023														
			Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre			
1	Revisar y actualizar el inventario de activos de información y su clasificación en los 16 procesos de la entidad dentro de la matriz de activos de información.	Inventario de activos actualizado															
2	Revisar y actualizar la matriz de los requisitos de orden jurídico (legales, regulatorios y reglamentarios) junto a los de tipo organizacional, técnico y contractual, incluyendo las partes interesadas de donde éstos surgen.	Matriz de requisitos legales actualizada															
3	Revisar y actualizar la metodología de gestión de riesgos de seguridad de la información, así como la matriz de riesgos, en cuanto a los riesgos identificados y su valoración, junto a la revisión de eficacia de controles establecidos alineado al Anexo A.	Metodología de riesgos actualizada. Matriz de riesgos (y sus controles) actualizada															
4	Actualizar el Manual con las políticas y lineamientos para la seguridad y privacidad de información, gestionar su aprobación y socializarlas.	Documento Manual de políticas de seguridad de la información actualizado, aprobado y socializado.															
5	Revisar y actualizar procedimientos de seguridad de la información, así como generar los adicionales que sean necesarios (siempre que sean estos)	Procedimientos del SGSI aprobados															

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 02	<b>Página:</b> 12 de 13
		<b>Vigente desde:</b> 20/01/2022	

	críticos para la organización), gestionar la aprobación y realizar su divulgación.																		
6	Revisar el plan de comunicación, sensibilización y capacitación SGSI.	Plan de comunicación, sensibilización y capacitación actualizado.																	
7	Revisar y actualizar las metodologías y herramientas de gestión de eventos e incidentes con base en su eficacia.	Documentación actualizada de gestión de eventos e incidentes de seguridad.																	
8	Realizar seguimiento a la aplicación oportuna (periódica o por evento) de los controles establecidos en el plan de tratamiento de riesgos. Presentar los informes periódicos de seguimiento de riesgos de seguridad de la información incluyendo datos sobre la eficacia de los controles.	Informes periódicos de seguimiento de riesgos en los cuales se incluyen los riesgos de seguridad de la información.																	
9	Realizar una evaluación continua de las competencias en gestión segura de la información para cada una de las funciones y roles en la entidad. Mantener actualizado el programa de desarrollo y fortalecimiento de las competencias técnicas y de gestión (capacitación) y toma de conciencia, junto a la evaluación de su eficacia.	Programa de desarrollo y fortalecimiento de las competentes y toma de conciencia en el SGSI. Evidencia de acciones de formación y evaluación de su eficacia.																	
10	Realizar la medición y análisis de datos en los indicadores de gestión de seguridad de la información.	Fichas de indicadores, con datos y análisis de patrones y tendencias																	
11	Proyectar y aprobar el documento con el Plan de seguimiento y revisión del SGSI.	Documento con el Plan de seguimiento y revisión del SGSI aprobado.																	
12	Ejecución de auditorías programadas (interna) al Sistema de Gestión de la Seguridad de la Información (SGSI) según el programa de auditoría.	Reportes de auditoría Programa de auditoría																	

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

<b>PERSONERÍA DE BOGOTÁ, D. C</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-PL-06</b>	
		<b>Versión:</b> 02	<b>Página:</b> 13 de 13
		<b>Vigente desde:</b> 20/01/2022	

		Planes de acción frente a posibles no conformidades																
13	Realizar la revisión por la dirección al SGSI asegurando la incorporación de las entradas y salidas definidas en la norma ISO/IEC 27001.	Actas de revisión por la dirección																

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.