
 <p><b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE</p>	<b>GESTION OPERATIVA DE TECNOLOGIAS DE LA INFORMACIÓN</b>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b>	FECHA: 31/01/2022
		Página 1 de 10

### Tabla de Contenido

1.	INTRODUCCIÓN	2
2.	OBJETIVO GENERAL:	2
3.	OBJETIVOS ESPECÍFICOS	2
4.	ALCANCE	3
5.	ROLES Y RESPONSABILIDADES	3
5.1.	Comité Institucional de Gestión y Desempeño	3
5.2.	Oficina de Tecnologías de la Información	3
5.3.	Líderes y Gestores de Procesos y Dependencias	3
5.4.	Funcionarios Públicos y Contratistas	3
6.	MARCO NORMATIVO	3
7.	METODOLOGÍA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN:	4
7.1.	GENERALIDADES	4
7.2.	IDENTIFICACIÓN DE NECESIDADES	4
7.3.	CAPACIDAD ORGANIZACIONAL	5
7.4.	IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN	5
8.	ACTIVIDADES DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN - 2022	5
9.	TÉRMINOS Y DEFINICIONES	7
10.	CONTROL DE CAMBIOS	10
11.	RESPONSABLES DE ELABORACIÓN, REVISIÓN Y APROBACIÓN	10

 <p><b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE</p>	<p align="center"><b>GESTION OPERATIVA DE TECNOLOGIAS DE LA INFORMACIÓN</b></p>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<p align="center"><b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b></p>	FECHA: 31/01/2022
		Página 2 de 10

## 1. INTRODUCCIÓN

La implementación del plan de Seguridad de la Información en la Secretaría de Cultura, Recreación y Deporte – SCRD, tiene como finalidad fortalecer las necesidades, requisitos, y acciones en materia de seguridad, promoviendo así la implementación y apropiación de la cultura de seguridad de y protección de la información institucional, aplicando las recomendaciones y mejores prácticas de seguridad, definidas en las directrices y lineamientos del MSPI y en la norma ISO 27001 que aplica para la gestión e implementación de Sistemas de Gestión de Seguridad de la Información.

La Secretaría de Cultura, Recreación y Deporte – SCRD, determina la información, los recursos tecnológicos y humanos, como activos vitales para el desarrollo de sus funciones institucionales, de conformidad con la misión y la visión de la SCRD, así mismo, se demuestra el compromiso de la Alta Dirección con la seguridad de la información, teniendo en cuenta que este proceso es liderado y apoyado de forma permanente por la Oficina de Tecnologías de la Información.


El Modelo de Seguridad y Privacidad de la Información – MSPI, pertenece al habilitador transversal de la Política de Gobierno Digital, el cual se desarrolla a través del – MSPI, el cual está orientado a la gestión e implementación del Sistema de Gestión de Seguridad de la Información – SGSI, cuya finalidad es incorporar el componente de seguridad de la información en todos los procesos, dependencias, aplicativos, sistemas de información, infraestructura tecnológica, conectividad y se hace extensivo a todos los demás activos de información de la Secretaría de Cultura, Recreación y Deporte – SCRD, cuya finalidad es garantizar la confidencialidad, integridad y disponibilidad de la información.

## 2. OBJETIVO GENERAL:

Definir la hoja de ruta y las actividades que hacen parte de la implementación del Plan de Seguridad de la Información de la Secretaría de Cultura, Recreación y Deporte para la vigencia 2022, en el marco de las directrices del Modelo de Seguridad y Privacidad de la Información.

## 3. OBJETIVOS ESPECÍFICOS

- Identificar y proteger los activos de información de la Secretaría de Cultura, Recreación y Deporte.
- Identificar y gestionar los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- Fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información de la SCRD, mediante la implementación y mejora de los controles de seguridad alineados con el Modelo de seguridad y privacidad de la información y la ISO 27001:2013..
- Sensibilizar a los funcionarios públicos y contratistas de la SCRD, frente al Modelo de Seguridad y Privacidad de la Información, fomentando de esta forma el nivel de conciencia frente a la necesidad de proteger los activos de información críticos.
- Definir y divulgar las políticas, lineamientos, procedimientos y buenas prácticas recomendaciones para establecer una cultura organizacional de Seguridad y Privacidad de la Información en la SCRD.

 <p><b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE</p>	<b>GESTION OPERATIVA DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b>	FECHA: 31/01/2022
		Página 3 de 10

#### 4. ALCANCE

El Plan de Seguridad de la Información aplica a todos los procesos, dependencias, funcionarios públicos y contratistas de la SCRD, cuya finalidad es velar por establecer niveles apropiados de seguridad de los activos de información.

#### 5. ROLES Y RESPONSABILIDADES

##### 5.1. Comité Institucional de Gestión y Desempeño

- Es responsable de apoyar la gestión de recursos financieros, administrativos, apoyar iniciativas y proyectos, revisar y aprobar el Plan de Seguridad de la Información y de promover el compromiso y participación de funcionarios públicos y contratistas de la SCRD.

##### 5.2. Oficina de Tecnologías de la Información

- Es responsable de realizar seguimiento, revisión, actualización y mejora del Plan de Seguridad de la Información.

##### 5.3. Líderes y Gestores de Procesos y Dependencias


- Son responsables de gestionar y apoyar la ejecución e implementación de las acciones y/o controles definidos en el presente plan.

##### 5.4. Funcionarios Públicos y Contratistas

- Son responsables de participar en las actividades, sensibilizaciones, y demás actividades previstas en el presente plan.
- Mantener y garantizar la confidencialidad e integridad de la información.
- Cumplir las directrices, lineamientos y políticas definidos en el SGSI.

#### 6. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por medio del cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.

 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE	<b>GESTION OPERATIVA DE TECNOLOGIAS DE LA INFORMACIÓN</b>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b>	FECHA: 31/01/2022
		Página 4 de 10

NORMA	DESCRIPCIÓN
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
NTC/ISO 27001 de 2013	Sistemas de Gestión de Seguridad de la Información. Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio.

## 7. METODOLOGÍA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN:

La metodología de implementación del Plan de Seguridad de la Información de la Secretaría de Cultura, Recreación y Deporte, está basada en la aplicación del ciclo PHVA (Planear, Hacer, Verificar, y Actuar), de acuerdo con las directrices del Modelo de Seguridad y Privacidad de la Información - MSPI, ISO 27001:2013 y el Decreto 1008 del 14 de junio de 2018.


### 7.1. GENERALIDADES

El presente plan está orientado a mejorar por medio de la implementación acciones concretas al Sistema de Gestión de Seguridad y Privacidad de la Información de la SCRD; para tal fin es necesario mencionar que estas acciones están enmarcadas intervenir los 3 componentes del modelo (Personas, Procesos y Tecnología).

- **Compromiso:** Para la ejecución del plan es necesaria la participación de los diferentes niveles de decisión de la SCRD (estratégico, táctico y operativo), especialmente para la valoración de procesos frente a las normas ISO 27001/2:2013, así como también se asume el compromiso y el involucramiento de todos los colaboradores de la SCRD.
- **Población Objetivo:** Para asegurar el éxito en la ejecución del plan es prioritario involucrar a las personas que ejercen responsabilidades de seguridad de la información en la SCRD, así como también a todos los colaboradores que deben apoyar y/o asistir a las reuniones y entrevistas para el levantamiento de la información requerida y que por su actuar están directa o indirectamente relacionados con los procesos y procedimientos establecidos de Seguridad de la Información.
- **Duración:** El tiempo estimado para la ejecución del plan es de 11 meses contados a partir de la aprobación del presente plan de trabajo.

### 7.2. IDENTIFICACIÓN DE NECESIDADES

El Plan de Seguridad de la Información requiere de la designación, participación activa y constante de los actores clave (equipo de trabajo) de cada uno de los procesos y dependencias de la SCRD,

 <p><b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE</p>	<b>GESTION OPERATIVA DE TECNOLOGIAS DE LA INFORMACIÓN</b>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b>	FECHA: 31/01/2022
		Página 5 de 10

garantizando la comprensión e identificación del estado actual de la SCRD en materia de seguridad de la información, se identifican las necesidades que se requieren gestionar, para lograr una adecuada implementación del plan.

### 7.3. CAPACIDAD ORGANIZACIONAL

Partiendo de la identificación de las partes interesadas y la designación de los actores clave de cada proceso, es necesario evaluar la capacidad y estructura de los procesos oficiales que se encuentran definidos en el mapa de procesos de la SCRD, cuya finalidad es identificar tempranamente debilidades y obstáculos que permitan establecer las acciones a que haya lugar y se propicie el cumplimiento de los objetivos del plan.

### 7.4. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

La etapa de implementación se centra en la ejecución y cumplimiento de las actividades y objetivos acordados y aprobados, de la misma forma se tienen en cuenta los roles y responsabilidades y los tiempos de entrega por parte del equipo de trabajo involucrado en el Plan de Seguridad de la Información (todos los procesos, actores clave, equipo directivo). El resultado esperado de esta fase es la adecuada implementación y cumplimiento de las actividades previstas en el plan de Seguridad la Información - MSPI.

## 8. ACTIVIDADES DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN - 2022

Para que el modelo de seguridad y privacidad de la información continúe su implementación y operación de forma adecuada en la en la Secretaría de Cultura, Recreación y Deporte, se proponen las siguientes actividades para la vigencia 2022. En esta fase se definen las actividades y cronograma requeridos para la ejecución del Plan de Seguridad de la Información, entre los meses de Febrero a Diciembre de 2022.

Actividades del Plan de Seguridad de la Información - SCRD 2022				
Actividad	Resultados Esperados	Responsable	Fecha Inicial	Fecha Final
Definición y seguimiento del plan de seguridad y privacidad de la información 2022	Definición del Plan de Seguridad de la Información	Equipo de seguridad	20/01/2021	31/01/2022
	Seguimiento de planes I trimestre 2022	Equipo de seguridad	1/02/2022	1/04/2022
	Seguimiento de planes II trimestre 2022	Equipo de seguridad	1/04/2022	1/07/2022
	Seguimiento de planes III trimestre 2022	Equipo de seguridad	1/07/2022	1/10/2022
	Seguimiento de planes IV trimestre 2022	Equipo de seguridad	1/10/2022	20/12/2022
Revisión del Manual de Políticas de Seguridad y	Revisión del Manual de Políticas de Seguridad y Privacidad de la Información, se actualizará en caso ser necesario.	Equipo de seguridad	1/10/2022	30/11/2022

Si este documento se encuentra en medio digital fuera de la intranet de la Secretaría de Cultura, Recreación y Deporte, o es una copia impresa, se considera como COPIA NO CONTROLADA. Por favor piense en el medio ambiente antes de imprimir este documento



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE CULTURA,  
RECREACIÓN Y DEPORTE

**GESTION OPERATIVA DE TECNOLOGIAS DE LA  
INFORMACIÓN**

CÓDIGO: GOT-PN-02

VERSIÓN: 01


**PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD**

FECHA: 31/01/2022

Página 6 de 10

**Actividades del Plan de Seguridad de la Información - SCRD 2022**

Actividad	Resultados Esperados	Responsable	Fecha Inicial	Fecha Final
Privacidad de la Información				
Equipo Técnico de Gestión y Desempeño de Seguridad de la Información	Se realizará como mínimo un comité ETGD de Seguridad de la Información entre meses de febrero a noviembre 2022	Equipo de seguridad	1/02/2022	30/11/2022
Actualización inventario de activos de información	Identificar y/o actualizar de los activos de información	Equipo de seguridad /Todos los procesos y dependencias	1/02/2022	30/11/2022
	Registro de Activos de Información 2022	Equipo de seguridad /Todos los procesos y dependencias	1/10/2021	30/11/2022
	Índice de Información Clasificada y Reservada 2022	Equipo de seguridad /Todos los procesos y dependencias	1/10/2021	30/11/2022
Riesgos de Seguridad de la Información	Definir Manual de riesgos de seguridad de la información	Equipo de seguridad	1/02/2022	28/02/2022
	Apoyar la Identificación de los riesgos de Seguridad de las dependencias y procesos.	Todas las dependencias y procesos SCRD	1/06/2022	30/06/2023
Análisis de vulnerabilidades de la infraestructura TI	Remediación de vulnerabilidades 2021	Equipo de seguridad Equipo Infraestructura Equipo de desarrollo Oficina de Comunicaciones Oficina de Planeación	1/02/2022	28/02/2022
	Análisis y remediación de vulnerabilidades 2022 I cuatrimestre	Equipo de seguridad Equipo Infraestructura Equipo de desarrollo Oficina de Comunicaciones Oficina de Planeación	1/02/2022	30/04/2022
	Análisis y remediación de vulnerabilidades 2022 II cuatrimestre	Equipo de seguridad Equipo Infraestructura Equipo de desarrollo Oficina de Comunicaciones Oficina de Planeación	2/05/2022	31/08/2022

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE</p>	<b>GESTION OPERATIVA DE TECNOLOGIAS DE LA INFORMACIÓN</b>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b>	FECHA: 31/01/2022
		Página 7 de 10

Actividades del Plan de Seguridad de la Información - SCRD 2022				
Actividad	Resultados Esperados	Responsable	Fecha Inicial	Fecha Final
	Análisis y remediación de vulnerabilidades 2022 III cuatrimestre	Equipo de seguridad Equipo Infraestructura Equipo de desarrollo Oficina de Comunicaciones Oficina de Planeación	1/09/2022	30/12/2022
Plan de Capacitación y Sensibilización de Seguridad de la Información 2022	Seguimiento del plan I Semestre 2022	Equipo de seguridad	1/02/2022	30/06/2022
	Seguimiento del plan II Semestre 2022	Equipo de seguridad	1/07/2022	30/11/2022
Medición y Reportes de indicadores del SGSI	Oficialización de los indicadores del SGSI	Equipo de seguridad	1/02/2022	1/03/2022
	Reporte I semestre de indicadores del SGSI	Equipo de seguridad	1/03/2022	5/07/2022
	Reporte II semestre de indicadores del SGSI	Equipo de seguridad	1/07/2022	20/12/2022
Seguimiento y actualización del autodiagnóstico del MSPI	Seguimiento y actualización del autodiagnóstico del MSPI I semestre 2022	Equipo de seguridad	1/02/2022	30/06/2022
	Seguimiento y actualización del autodiagnóstico del MSPI II semestre 2022	Equipo de seguridad	1/07/2022	20/12/2022
Actualización RNBD	Registro Nacional de bases de datos personales	Equipo de seguridad /Todos los procesos y dependencias	1/02/2022	30/03/2022


## 9. TÉRMINOS Y DEFINICIONES

**Activo de Información:** Un activo de información es, cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse (ISO/IEC 27001:2013).

**Alta dirección:** Persona o grupo de personas que dirige y controla una organización, al nivel más alto (ISO/IEC 27001:2013).

**Amenaza:** Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas. Cuando el Agente de riesgo selecciona una víctima contra la cual pretende cometer un acto delictivo, automáticamente se convierte en una amenaza para ella. Se puede considerar que es la materialización del riesgo.

**Clasificación de la información:** Los responsables de los activos de información deben documentar la clasificación de seguridad de los activos de información de los cuales son responsables y designarán

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE</p>	<p><b>GESTION OPERATIVA DE TECNOLOGIAS DE LA INFORMACIÓN</b></p>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<p><b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b></p>	FECHA: 31/01/2022
		Página 8 de 10

un custodio para cada activo, a su vez éste será responsable de la implementación de los controles de seguridad.

La clasificación de la información de la Secretaría de Cultura, Recreación y Deporte se debe realizar con base en la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015 y la Ley 594 de 2000 (Ley General de Archivos).

**Compromiso de la Dirección:** Alineamiento firme de la Dirección de la SCRD con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de Seguridad de la Información.

**Confidencialidad:** El acceso a la información es permitido exclusivamente al personal autorizado, sin revelar la misma a terceras partes y/o personas.

**Custodio:** Es una parte designada de la SCRD, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. Tomado de [https://www.mintic.gov.co/gestionti/615/articles-482\\_G5\\_Gestion\\_Clasificacion.pdf](https://www.mintic.gov.co/gestionti/615/articles-482_G5_Gestion_Clasificacion.pdf)

**Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012 – Artículo 3).

**Disponibilidad:** En seguridad informática es un término hace referencia a la característica de poder acceder a la información en el momento que se requiera.

**Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad (NTC-ISO/IEC 27001 2013).


**Gestión de la seguridad en los activos:** La Secretaría de Cultura, Recreación y Deporte a través de los procesos Gestión Tecnológica y Gestión Administrativa deben establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información de tipo información, datos, software, hardware y servicios, con el objetivo de garantizar su protección.

**Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y su tratamiento. (ISO 27000, Glosario de términos y definiciones).

**Gobierno de seguridad de la información:** Es el conjunto de responsabilidades y prácticas ejercidas por el Grupo Directivo con el propósito de evaluar, dirigir, monitorear y comunicar todas las acciones y/o actividades relacionadas con la protección de la información de la SCRD. (ISO/IEC 27014:2013).

**Hardware:** Conjunto de equipos de cómputo, servidores, redes, equipos de seguridad, impresoras, scanner, equipos de almacenamiento, entre otros, que utiliza la Secretaría de Cultura, Recreación y



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE</p>	<b>GESTION OPERATIVA DE TECNOLOGIAS DE LA INFORMACIÓN</b>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b>	FECHA: 31/01/2022
		Página 9 de 10

Deporte.

**Impacto:** Resultado de un incidente de seguridad de la información.

**Incidente de seguridad:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Información:** Es un conjunto de datos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, USB, etc.).

**La información documentada:** (Inglés: Documented information). Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida

La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la organización funcione (documentación) y/o evidencias de resultados alcanzados (registros)

**Incidente:** Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información

**Inventario de activos:** Los responsables de la información deben propender para que se mantenga actualizado el inventario de sus activos de información y hagan entrega de éste al menos una vez al año. La consolidación de dicho inventario está bajo la responsabilidad de la Dirección de Gestión Administrativa.


**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

**Propietario de la Información:** Es una parte designada de la SCRD, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

**SGSI - Sistema de Gestión de Seguridad de la Información:** Según [ISO/IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.

**Seguridad de la Información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas (NTC-ISO/IEC 27001:2013).

**Software:** Conjunto de programas, sistemas operativos, aplicaciones de ofimática entre otros

 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE	<b>GESTION OPERATIVA DE TECNOLOGIAS DE LA INFORMACIÓN</b>	CÓDIGO: GOT-PN-02
		VERSIÓN: 01
	<b>PLAN DE SEGURIDAD DE LA INFORMACIÓN SCRD</b>	FECHA: 31/01/2022
		Página 10 de 10

aplicativos propios y/o tercerizados que utiliza la Secretaría de Cultura, Recreación y Deporte.

**Terceros:** Personas que no son empleados de la Secretaría de Cultura, Recreación y Deporte o empresas diferentes al mismo. Ejemplo: Participantes, beneficiarios, proveedores regulares o potenciales de bienes y servicios, empresas candidatas a prestar servicios a la Secretaría de Cultura, Recreación y Deporte, entes reguladores, consultores, etc.

**Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

## 10. CONTROL DE CAMBIOS

Nota: A partir de la aprobación del mapa de procesos versión 09, se reinicia el versionamiento documental esto quiere decir, que inicia en la versión 01, teniendo en cuenta el rediseño institucional, la nueva codificación buscando la simplificación de documentos.

Versión	Cambios realizados
1	Solicitud inicial. Ver "Solicitud de elaboración, modificación o eliminación de documentos" Fecha: 27/01/2022 Radicado ORFEO.

## 11. RESPONSABLES DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORÓ	REVISÓ OAP	REVISÓ	APROBÓ *
NOMBRE: Andrés Cadena	NOMBRE: Angelmiro Vargas	NOMBRE: Yaneth Suárez Alba Nohora Díaz Omar Urrea Romero Nidia Miranda Sonia Córdoba Liliana Morales	NOMBRE: Comité Institucional de Gestión y Desempeño de la SCRD
CARGO: Contratista Oficina de Tecnologías de la Información	CARGO: Profesional Universitario	CARGO: Directora Corporativa Coordinador GIT GTH Jefe OCI Coordinador GITGSA Jefe OAP Jefe OTI	CARGO: N/A
FIRMA: Electrónica	FIRMA: Electrónica	FIRMA: Electrónica	FIRMA: Electrónica

\* Aprobado por el Comité Institucional de Gestión y Desempeño, en sesión del 31/01/2021.