



**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN BOMBEROS DE  
BUCARAMANGA**

Código: PL-GT-SGC-110-003

Versión: 1.0

Página 1 de 18

**Contenido**

1. OBJETIVO	2
2. OBJETIVOS ESPECIFICOS	2
3. ALCANCE	2
4. RESPONSABLE	2
5. GLOSARIO	3
6. CONDICIONES GENERALES	7
7. DOCUMENTOS DE REFERENCIA	8
8. MARCO LEGAL	8
9. DESARROLLO	9
10. CRONOGRAMA DE ACTIVIDADES	17
11. HISTORIAL DE CAMBIOS	18

**EXCELENCIA Y COMPROMISO**

Sede Administrativa: Calle 44 Número 10 -13  
Bucaramanga, Santander  
PBX: 6526666 Línea Emergencias 119 – 123  
Telefax: Dirección General: 6522220

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 2 de 18

## 1. OBJETIVO

Describir las actividades del plan de Seguridad y Privacidad de la Información, con las cuales se busca cumplir los lineamientos que respondan eficazmente a eventos que afecten la seguridad de la información, así como asegurar la continuidad de los procesos soportados por TI.

## 2. OBJETIVOS ESPECIFICOS

- Implementar el modelo de Seguridad y Privacidad de la información, con el fin de cumplir con los lineamientos del componente de Seguridad y Privacidad de la información y aplicar la seguridad de la información al interior de Bomberos de Bucaramanga.
- Identificar las aplicaciones y los activos considerados críticos para la operación de Bomberos de Bucaramanga entorno a los servicios de TI.
- Establecer los tiempos mínimos de recuperación de servicios de TI requeridos en los que no se vea afectado la operación de la entidad.

## 3. ALCANCE

La estructura del Plan se basa en la temática propuesta por el Ministerio de las Tecnologías de la información y las Comunicaciones MINTIC para el componente de Seguridad y Privacidad de la información, como para la continuidad de TI.

Dentro de la gestión de TI se quiere garantizar que el Plan aplique para todos los procesos.

## 4. RESPONSABLE

### EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 3 de 18

Dirección Administrativa y financiera

## 5. GLOSARIO

**Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

**Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

**Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

**Control:** son todas y cada uno de las medidas preventivas que se toman para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Con el fin de salvaguardar la información. En una definición más simple, es una medida que modifica el riesgo.

**Confidencialidad:** Que la información solo sea vista por personal autorizado

**Datos personales privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular (Ley 1266 de 2008, art 3).

**Datos personales públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no sometidas a reserva. (Decreto 1074 de 2015, art 2.2.2.25.1.3.).

## EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 4 de 18

**Datos Personales Privados:** Es el dato personal que por su naturaleza íntima o reservada sólo le interesa al titular y para su tratamiento requiere autorización expresa del titular.

**Datos personales semiprivados:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios ((Ley 1266 de 2008, art 3).

**Datos personales sensibles.** entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a vida sexual, y datos biométricos (Decreto 1074 de 2015, art 2.2.2.25.1.3.).

**Declaración de aplicabilidad:** Documento que enlista los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los diferentes procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

**Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

**Disponibilidad:** Asegurar que la información esté disponible.

**Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

### **EXCELENCIA Y COMPROMISO**

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 5 de 18

**Gestión de incidentes de seguridad de la información:** Conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una Entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.

**Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

**Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

**Información Pública:** Es aquella información que puede ser obtenida y ofrecida sin alguna reserva a cualquier persona dentro y fuera de la entidad y sin importar si la misma sea información general, sin que eso dañe a procesos propios de la entidad.

**Integridad:** Datos originales. Garantizar que la información no sea modificada.

**Interrupción:** Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar una interrupción de los procesos de la entidad o calidad del servicio.

**Plan de Continuidad del Negocio:** documento que describe los procesos y procedimientos que una entidad u organización pone en marcha para garantizar que las principales funciones misionales o del negocio puedan continuar durante y después de un desastre.

## EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 6 de 18

**Plan de tratamiento de riesgos** Es un documento que define las acciones para seleccionar y aplicar las medidas más adecuadas, con el fin de mitigar los riesgos de seguridad de la información inaceptables, o bien aprovechar las ventajas que pueda reportarnos.

**Punto objetivo de recuperación (RPO).** Punto en el tiempo en el cual los archivos deben ser recuperados del almacenamiento de copias de seguridad después de que una interrupción ocurra.

**Punto Tiempo objetivo de tiempo de recuperación (RTO).** Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra para la continuidad del servicio.

**Privacidad:** se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias la obligación de proteger dicha información teniendo en cuenta las Leyes que la soportan.

**Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos (Ley 1581 de 2012, art 3).

**Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

**Riesgo De Seguridad De La Información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información, Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se

### **EXCELENCIA Y COMPROMISO**

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 7 de 18

genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

**Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

**Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la Disponibilidad de la información, además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

**Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento (Ley 1581 de 2012, art 3).

**Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ley 1581 de 2012, art 3).

## 6. CONDICIONES GENERALES

La Dirección Administrativa y Financiera, con la unidad de apoyo de telemática y Hábeas Data, administrará los riesgos de seguridad de la información para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información institucional y personal.

La Dirección Administrativa y Financiera, con la unidad de apoyo de telemática y Hábeas Data, continuará monitoreando la debida actualización al inventario de activos de información institucional y personal por parte de cada proceso o área, definiendo al área o proceso de TI quien recopila la información generando un solo documento con todos los activos de la entidad.

La Dirección Administrativa y Financiera, con la unidad de apoyo de telemática y Hábeas Data, continuará monitoreando la debida actualización al inventario de

## EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 8 de 18

la información clasificada y reservada, confidencial semiprivada, privada o sensible teniendo en cuenta la legislación colombiana.

## 7. DOCUMENTOS DE REFERENCIA

- Documento CONPES 3995. Política Nacional de Confianza y Seguridad Digital.
- Guía modelo de seguridad y privacidad de la información. Ministerio de las TIC.
- Manual de Gobierno Digital. Implementación del Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2).
- Subtítulo 2.4. y subtítulo 2.6. de la Guía de para la Implementación del Principio de Responsabilidad Demostrada (Accountability). Superintendencia de Industria y Comercio.
- Política de Tratamiento de Datos Personales de Bomberos de Bucaramanga. Resolución 208 de noviembre de 2019.

## 8. MARCO LEGAL

- Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. (Integrado en el Decreto Único Reglamentario 1074 de 2015).
- Manual estrategia de Gobierno en Línea.

## EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 9 de 18

- Decreto 1008 del 2018. Por el 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 620 de 2020. Por el cual se establecen los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

## 9. DESARROLLO

### 9.1. Política de seguridad de la información de Bomberos de Bucaramanga.

BOMBEROS DE BUCARAMANGA se compromete a administrar los riesgos de seguridad de la información institucional y personal para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de los requisitos aplicables. De igual manera, promueve una cultura en seguridad para evitar y administrar incidentes que contribuyan a cada uno de los procesos tanto internos como externos de la entidad.

### 9.2. Plan desarrollado de seguridad y privacidad de la información y continuidad de TI.

BOMBEROS DE BUCARAMANGA ha realizado el Plan de Seguridad de la Información y continuidad de TI que permita cumplir con el objetivo definido en dicho plan, con esto definimos las actividades que se describen a continuación:

#### 9.2.1. Realizar el inventario de activos de información.

Realizar monitoreo y actualización al inventario de activos de información por parte de cada proceso o área, definiendo al área o proceso de TI quien recopila la información generando un solo documento con todos los activos de la entidad, lo anterior con el fin de definir la criticidad, los dueños de cada proceso, custodios y usuarios.

## EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 10 de 18

Así mismo se tendrá en cuenta la Guía No. 5. Gestión Clasificación de Activos la cual brinda y asesora en cómo llevar a cabo todas las actividades mencionadas con anterioridad. [http://www.mintic.gov.co/gestioni/615/articles-5482\\_G5\\_Gestion\\_Clasificacion.pdf](http://www.mintic.gov.co/gestioni/615/articles-5482_G5_Gestion_Clasificacion.pdf).

### 9.2.2. Inventario de información clasificada y reservada

Realizar monitoreo y actualización al inventario de la información clasificada y reservada o confidencial teniendo en cuenta su importancia, se hace necesario que Bomberos de Bucaramanga aplique los debidos controles para el cuidado o preservación de la información, así como para su almacenamiento y disposición final. Para estructurar este Plan se tiene en cuenta la guía para la gestión y Clasificación de Activos de Información.<sup>1</sup>

### 9.2.3. Declaración de aplicabilidad

Cuando se haya aprobado los documentos relacionados con los riesgos de seguridad se debe elaborar el documento de la declaración de aplicabilidad que enmarca los controles aplicables para la seguridad de la información, se debe indicar si los objetivos y los controles aplican para Bomberos de Bucaramanga y se debe justificar cada uno de ellos teniendo en cuenta los que no se incluyan. La declaración de aplicabilidad debe ser revisada antes cambios significativos de los elementos de la plataforma tecnológica y/o personal. Esta información, se debe revisar y aprobar.

### 9.2.4. Categorización de los Servicios de TI

Realizar el levantamiento de los servicios apoyados por TI, para medir el nivel de cada actividad soportada por TI, es crítica para Bomberos de Bucaramanga y necesita contar con un plan para su reanudación, las anteriores actividades deberán contar con un tiempo objetivo de recuperación (RTO) y un punto objetivo de

<sup>1</sup> MINTIC GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN:  
[https://www.mintic.gov.co/gestioni/615/articles-5482\\_G5\\_Gestion\\_Clasificacion.pdf](https://www.mintic.gov.co/gestioni/615/articles-5482_G5_Gestion_Clasificacion.pdf)

**EXCELENCIA Y COMPROMISO**

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 11 de 18

recuperación (RPO) para la meta mínima de continuidad de TI por producto o Servicio.

### 9.2.5. Definición de estrategias de continuidad de TI

Con el fin de mantener los principios de prevención de incidentes, detección, respuesta, recuperación y restauración de los productos y servicios soportados por TI y que se pongan en marcha en Bomberos de Bucaramanga, primero deberán ser aprobadas por la alta dirección y sensibilizadas al interior de Bomberos de Bucaramanga.

### 9.2.6. Plan de capacitación, comunicaciones y sensibilización de seguridad y privacidad de la información.

Bomberos de Bucaramanga debe implementar un plan de comunicación, sensibilización que incluya la estrategia para que la seguridad de la información se convierta en cultura institucional, al generar competencias y hábitos en toda la entidad, para estructurar este plan se toma como base la guía No. 14 – Plan de Comunicación, Sensibilización y Capacitación<sup>2</sup> este plan se encontrará anexo a este documento.

### 9.2.7. Plan de transición de IPv4 a IPv6

Teniendo en cuenta los lineamientos que dicta el Ministerio de las tecnologías de la información y las Comunicaciones (min TIC) y así cumplir los objetivos de innovación tecnológica que exige el país, donde todas las entidades deben entrar a un plan de transición del protocolo de IPv4 al nuevo protocolo IPv6.

Lo anterior tomando como base la Guía No. 20 transición de IPv4 a IPv6<sup>3</sup>. ([http://www.mintic.gov.co/gestioni/615/articles-5482\\_Guia23\\_Transicion\\_IPV4\\_IPV6.pdf](http://www.mintic.gov.co/gestioni/615/articles-5482_Guia23_Transicion_IPV4_IPV6.pdf)).

### 9.2.8. Indicadores de gestión de la seguridad de la información

<sup>2</sup> MINTIC PLAN DE COMUNICACIONES [http://www.mintic.gov.co/gestioni/615/articles-5482\\_G14\\_Plan\\_comunicacion\\_sensibilizacion.pdf](http://www.mintic.gov.co/gestioni/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf)

<sup>3</sup> MINTIC IPV6 [http://www.mintic.gov.co/gestioni/615/articles-5482\\_G20\\_Transicion\\_IPv4\\_IPv6.pdf](http://www.mintic.gov.co/gestioni/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf)

## EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 12 de 18

Generar o actualizar los indicadores de gestión a la medición de la efectividad, eficiencia y eficacia en el modelo de operación del marco de seguridad y privacidad de la información.

### 9.3. Cronograma de actividades

A continuación, se describen las actividades para el Plan de trabajo de Seguridad y privacidad de la información:

COMPONENTE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Objetivo	Documentos	Estado	Tareas	Fecha de Inicio
<b>DEFINICIÓN DEL MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DE LOS SISTEMAS DE INFORMACIÓN</b>	Busca definir el estado actual del nivel de seguridad y privacidad y define la implementar				
<b>Plan de seguridad y privacidad de la información</b>	Busca generar un plan de seguridad y privacidad alineado con el propósito	Plan de comunicación, sensibilización y capacitación (Anexo al plan de seguridad y Privacidad)	En revisión	a. Desarrollar las actividades relacionadas en el anexo del presente documento	23/06/2021
<b>IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Busca desarrollar las acciones definidas en el plan de seguridad y privacidad				

### EXCELENCIA Y COMPROMISO



**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN BOMBEROS DE  
BUCARAMANGA**

Código: PL-GT-SGC-110-003

Versión: 1.0

Página 13 de 18

Y DE LOS SISTEMAS DE INFORMACIÓN					
<b>Gestión de Riesgos Seguridad y Privacidad de la información</b>	Busca proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.	Documento con la estrategia de planificación y control operacional	para construcción	a. Elaborar la propuesta para la estrategia de planificación y control operacional  b. Solicitar la Aprobación del documento por la Alta Dirección (Gestión de TI)	21/07/2021
	Informe de la ejecución del plan de tratamiento de riesgos	para construcción	a. Realizar informes trimestrales de la ejecución del plan, luego de aprobado el Plan de tratamiento de riesgos	28/07/2021	

**EXCELENCIA Y COMPROMISO**

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 14 de 18

#### 9.4. Evaluación y seguimiento

Una vez implementadas las anteriores actividades, el Plan de Seguridad y Privacidad de la Información, se debe evaluar anualmente para medir la efectividad de las acciones tomadas a través de los indicadores definidos anteriormente, que permitan evaluar la interacción entre el modelo de seguridad y privacidad de la información y la aplicación de la Ley de Transparencia y Acceso a la Información Pública.

#### 9.5. Descripción general del plan de capacitación, sensibilización y comunicación

Bomberos de Bucaramanga ha estructurado el plan de Sensibilización de Seguridad y Privacidad de la Información que busca que todos los funcionarios y colaboradores cumplan con la Política de Seguridad y privacidad de la Información mediante actividades, capacitaciones, talleres y socializaciones.

El plan será diseñado e implementado para seguir los requerimientos exigidos por Gobierno Digital.

##### 9.5.1. Diseño del plan de capacitación, sensibilización y comunicación.

Para el diseño del plan se detallan los medios y herramientas de comunicación que se tendrán en cuenta para la ejecución del plan:

No	Medios y Herramientas
1	Folletos
2	Correo Masivo

### EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 15 de 18

Todos los funcionarios deben ver la información entregada de sensibilización como una responsabilidad compartida, en la actual vigencia algunos temas serán los siguientes:

- Administración de Contraseñas.
- Política de Seguridad de la Información
- Seguridad de la Información en el puesto de Trabajo
- Seguridad para los dispositivos USB
- Medidas de seguridad para la información clasificada y reservada
- Gestión de Incidentes (como reportar, que puedo reportar)
- Amenazas y Vulnerabilidades Comunes.

Las fuentes de información pueden ser de conferencias de seguridad, boletines de CSIRT-PONAL, organizaciones relacionadas con seguridad de la información, todos estos temas serán presentados a través de los medios descritos anteriormente.

### **9.5.2. Materiales para el plan de capacitación, sensibilización y comunicación.**

- Infraestructura: Las actividades de capacitación y socialización se desarrollarán en las instalaciones de Bomberos de Bucaramanga en la sala de Juntas, sala de Crisis o por correo electrónico, teniendo en cuenta las directrices impartidas por la actual situación de COVID-19.
- Equipo y otros: conformado por los equipos multimedia, video Beam, portátil, etc.

### **9.5.3. Instrumentos de sensibilización**

Con el apoyo de comunicaciones internas se requiere diseñar una estrategia de comunicación para sensibilizar al personal de Bomberos de Bucaramanga en temas de seguridad de la información y dar cumplimiento a la estrategia de Gobierno Digital, para lograr este fin se requiere de las siguientes actividades.

## **EXCELENCIA Y COMPROMISO**



## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA

Código: PL-GT-SGC-110-003

Versión: 1.0

Página 16 de 18

- Identificar con una imagen y nombre que represente los temas de seguridad y privacidad de la información.
- Captar la atención de los funcionarios y colaboradores de Bomberos de Bucaramanga para que participen con las actividades de seguridad y privacidad de la información.
- Entrega de folletos para los casos que se requieran.
- Socializar los videos de seguridad de la información, disponibles en la página de [enticconfio.gov.co](http://enticconfio.gov.co).

### 9.5.4. Acciones para la comunicación y sensibilización.

- Temario: Política de Seguridad y Privacidad de la Información
- Responsables: Dirección Administrativa y Financiera – unidad de apoyo de Telemática.
- Metodología a utilizar: Correos masivos.

### 9.6. Logros esperados

- Comprometer a todos los funcionarios y contratistas con la seguridad de la información.

### 9.7. Instrumentos de medición

Para medir la percepción de la Seguridad y Privacidad de la Información, se diseñarán encuestas que se aplicarán por lo menos dos veces al año con el fin de determinar que se debe mejorar en el plan.

## EXCELENCIA Y COMPROMISO



**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN BOMBEROS DE  
BUCARAMANGA**

Código: PL-GT-SGC-110-003

Versión: 1.0

Página 17 de 18

## 10. CRONOGRAMA DE ACTIVIDADES

No.	Actividad	Objetivos	Medios	Fecha de Ejecución	Frecuencia
1	Diseñar la estrategia para la campaña de sensibilización y comunicación con el apoyo de comunicaciones internas	Generar una campaña efectiva en donde los funcionarios participen activamente	Definido por comunicaciones internas	Segundo semestre 2021	
2	Socialización Política de Seguridad de la Información,	Lograr que todos en Bomberos de Bucaramanga conozcan sus responsabilidades de seguridad de la información	Correo.	Segundo semestre 2021	1 vez al año o cuando se requiera
3	Boletines informativos	Informar acerca de las últimas amenazas informáticas y la forma de contrarrestar	Correo	Primer-Segundo semestre 2021	Mensual
4	Encuestas de Seguridad de la Información	Conocer el grado de conocimiento adquirido de acuerdo a las actividades realizadas en seguridad de la información	Correo Masivo (Encuesta)	Segundo semestre 2021	Mínimo una vez al año

### EXCELENCIA Y COMPROMISO

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BOMBEROS DE BUCARAMANGA</b>	Código: PL-GT-SGC-110-003
		Versión: 1.0
		Página 18 de 18

## 11. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Se crea el documento.	Junio 11 de 2020
1.0	Se cambia el encabezado de acuerdo a la modificación del instructivo de documentos y se actualiza el cronograma de actividades.	Agosto 26 de 2020

## EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13  
 Bucaramanga, Santander  
 PBX: 6526666 Línea Emergencias 119 – 123  
 Telefax: Dirección General: 6522220