PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Cuerpo Oficial de Bomberos
BUCARAMANGA

VIGENCIA
2024

1. INTRODUCCIÓN

BOMBEROS DE BUCARAMANGA mediante la adopción e implementación del Plan de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo así por el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones - TIC, a través de políticas y programas.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

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.

2.2 OBJETIVOS ESPECÍFICOS

- 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

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 modificael riesgo.

Confidencialidad: Que la información solo sea vista por personal autorizado

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 riesgosy su justificación, así como la justificación de las exclusiones de controles del anexo Ade ISO 27001. (ISO/IEC 27000).

Disponibilidad: Asegurar que la información esté disponible.

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.

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.

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 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.

6. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Este proceso permitirá garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en Bomberos De Bucaramanga, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.

Ciclo PHVA del proceso de Seguridad y Privacidad

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

7. Asegurar la confidencialidad, integridad y disponibilidad de la información en la gestión y control de la prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones.

OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI.

8.

Modelo de Operación por Gestiones de Seguridad y Privacidad de la Información, seguridad digital y continuidad de la Operación

9. CONDICIONES GENERALES

La Dirección Administrativa y Financiera con el 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.

La Dirección Administrativa y Financiera con el apoyo de telemática y Hábeas Data, continuará monitoreando la debida 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.

La Dirección Administrativa y Financiera con el apoyo de telemática y Hábeas Data continuará monitoreando la debida actualización al inventario de la información clasificada y reservada o confidencial teniendo en cuenta su importancia.

10. DOCUMENTOS DE REFERENCIA

- Modelo de seguridad y Privacidad de la información MINTIC.
- Política de Tratamiento de datos personales de Bomberos de Bucaramanga. Resolución 208 de noviembre de 2019.
- Manual de Procedimientos para el Tratamiento de Datos Personales

11. MARCO LEGAL

Manual estrategia de Gobierno en Línea.

- 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 delsector de Tecnologías de la Información y las Comunicaciones.
- Resolución 2999 del 2008. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.

12. DESARROLLO

12.1.1 Política de seguridad de la información de Bomberos de Bucaramanga.

BOMBEROS DE BUCARAMANGA, se compromete a administrar los riesgos de seguridad de la información 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.

12.1.2 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:

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: +576076526666 Línea Emergencias 119
Telefax: Dirección General: +576076522220

12.1.3 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.

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/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf.

12.1.4 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.

[1] MINTIC GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN:https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

12.1.5 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[2] este plan se encontrará anexo a este documento.

12.1.6 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.

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: +576076526666 Línea Emergencias 119
Telefax: Dirección General: +576076522220

Lo anterior tomando como base la Guía No. 20 transición de IPv4 a IPv6[3]. (http://www.mintic.gov.co/gestionti/615/articles-5482_Guia23_Transicion_IPV4_IPV6.pdf).

[2] MINTIC PLAN DE COMUNICACIONES http://www.mintic.gov.co/gestionti/615/articles 5482_G14_Plan_comunicacion_sensibilizacion.pdf
MINTIC IPV6 http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

12.2 Cronograma de actividades

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

COMPONENTE SEGURIDAD Y PRIACIDAD DE LA INFORMACIÓN	OBJETIVO	Documentos	Estado	Tareas	Fecha de Inicio	Fecha de Finalización
DEFINICIÓN DEL MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DE LOS SISTEMAS DE INFORMACIÓN	**Busca definir el estado actual del nivel de seguridad y privacidad y define las acciones a implementar**					
Plan de seguridad y Privacidad de la información.	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	Construido anexo en este Plan	a. Desarrollar las actividades relacionadas en el Anexo del presente documento	01/02/2024	29/12/2024
IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DE LOS SISTEMAS DE INFORMACIÓN	**Busca desarrollar las acciones definidas en el plan de seguridad y privacidad.**					
Gestión de Riesgos de Seguridad y Privacidad de la Información	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)	04/03/2024	12/04/2024
		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.	08/04/2024	30/12/2024

Socialización de Buenas prácticas para la Seguridad de la Información.	Mitigar los riesgos de pérdida de información por desconocimiento de los usuarios de la entidad.	Capacitación en Tips de Ciberseguridad	Para construcción	Realizar capacitaciones Trimestrales al personal en general sobre Tips para proteger la información	19/02/2024	30/12/2024
Activos de información	Actualización de activos de información Ley 1712	Activos de información en formato Excel	Pendiente	a. solicitar a la unidad gestora oficina Juridica por correo electrónico los activos de información y si han cambiado realizar su actualización.	01/03/2024	05/04/2024
		Página web entidad	Pendiente	b. terminado la actualización del documento se debe subir a la página de la entidad.	11/04/2024	22/04/2024
Información clasificada y reservada	Actualización de información clasificada y reservada Ley 1712	Información clasificada en formato excel	Pendiente	a. solicitar a la unidad gestora oficina Jurídica por correo electrónico los activos de información y si han cambiado realizar su actualización.	01/03/2024	05/04/2024
		Página web entidad	Pendiente	b. terminado la actualización del documento se debe subir a la página de la entidad.	11/04/2024	22/04/2024
Actualización del Plan de capacitación, comunicaciones y sensibilización de seguridad y privacidad de la información	Documento actualizado	Construido	Para revisión	Ejecutar en plan con sus actividades	01/02/2024	30/12/2024
Plan de Transición IP4 a IPV6	fase II plan de Transición acordecon los lineamientos de MINTIC	Inventario de TI (hardware y Software), identificando cuales equipos soportan IPV6	Para Revisión	a. Revisar las cotizaciones que realizaron con los operadores de servicios, LACNIC y continuar con la implementación. Revisar el cableado estructurado de la entidad y mejorar los puntos de red.	01/05/2024	31/07/2024

12.2 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.

12.2.1 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, encuestas y socializaciones.

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

12.2.2 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

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
- 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 puedes 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.

12.2.2.1 Materiales para el plan de capacitación, sensibilización y comunicación.

Infraestructura: Las actividades de capacitación y socialización se desarrollarán por correo electrónico.

12.2.2.2 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.

- 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 https://colombiaaprende.edu.co/contenidos/plataforma/en-tic-confio.

12.2.2.3 Acciones para la comunicación y sensibilización

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

12.2.2.4 Logros esperados

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

12.2.2.5 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.

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	Primer semestre 2024	Única vez

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 2024	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 2024	Bimestral
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 2024	Mínimo una vez al año

13. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Creación del documento	2020/03/02
1.0	Se cambia el encabezado de acuerdo a la modificación del instructivo de documentos y se le agrega al plan el punto 5 que habla de condiciones generales.	Junio 11 de 2020
2.0	Se actualiza el documento y cronograma de actividades.	Enero de 2023
3.0	Se actualiza el documento y cronograma de actividades	Enero de 2024