

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Código: M-GT-SGC-200-001
			Versión: 0.0
			Fecha Aprobación: 13/04/2023
			TRD 200-32.14
			Página 1 de 23

Contenido

DERECHOS DE AUTOR.....3

AUDIENCIA.....4

INTRODUCCIÓN.....5

GLOSARIO.....6

OBJETIVOS.....11

Objetivo General.....11

Objetivos Específicos.....11

ALCANCE.....11

MARCO LEGAL.....12

CONOCIMIENTO DE LA INSTITUCION.....12

Misión.....12

Visión.....12

Valores Institucionales.....12

ORGANIGRAMA DEL CUERPO OFICIAL DE BOMBEROS.....13

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....14

CICLO PHVA (PLANEAR, HACER, VERIFICAR Y ACTUAR).....14

Planear.....15

Hacer.....15

Verificar.....15

Actuar.....16

DESCRIPCION DEL CICLO DE OPERACIÓN.....16

Diagnostico.....16

Planificación.....17

Implementación.....18

Evaluación de desempeño.....19

Mejora continua.....20

MODELO DE MADUREZ.....21

ADOPCION DEL PROTOCOLO IPV6.....24

Planeación.....24

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 2 de 23	

Implementación.....	24
Pruebas de funcionalidad.....	25
Firmas y revisiones.....	26
Control de cambios.....	26

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 3 de 23	

DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

AUDIENCIA

El Modelo de Privacidad y Seguridad de la Información está orientado a Bomberos de Bucaramanga y son de obligatorio cumplimiento en los procesos que sean referenciados en el Alcance y por todos los servidores públicos, proveedores, ciudadanos, terceros y demás personas vinculadas que hacen parte de dichos procesos.

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Código: M-GT-SGC-200-001
			Versión: 0.0
			Fecha Aprobación: 01/03/2023
			TRD 200-28.11
			Página 4 de 23

INTRODUCCIÓN

El 28 de Junio de 1943 la Asamblea de Santander aprobó la ordenanza 59, por la cual se ordenaba la creación de un Cuerpo de Bomberos de Santander, independiente de la Policía Departamental, estableciéndose los empleos que conformarían dicho cuerpo: un comandante, dos sargentos, dos cabos, veinticuatro bomberos, un motociclista y dos conductores.

La separación de este Cuerpo de Policía de Santander es una indicación de que previamente existía en la Policía una fuerza de tarea para la extinción de incendios, cuyo inventario de equipos se traspasó al nuevo Cuerpo creado.

El cuerpo oficial de bomberos de Bucaramanga es una entidad creada por el gobierno nacional para garantizar la seguridad de los ciudadanos por lo que es la encargada de cubrir toda situación irregular que ponga en riesgo la vida de las personas e incluso la de los animales.

Dicho lo anterior como una entidad que garantiza la seguridad ha identificado la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones, por lo que es indispensable la implementación del modelo de seguridad y privacidad de la información -MSPI, con la finalidad de preparar la entidad para la preservación de la confidencialidad, integridad y disponibilidad de los datos garantizando la privacidad y brindando confianza a las partes interesadas acerca de la aplicación de la gestión de riesgo.

Con la implementación de un modelo de seguridad y privacidad de la información MSPI, el cuerpo oficial de bomberos de Bucaramanga, busca establecer la seguridad para prevenir incidentes con un impacto negativo en el manejo de los datos logrando respetar los derechos de los titulares de los datos (privacidad) y optimizando la labor de acceso a la información pública.

Este documento se elaboró siguiendo los lineamientos del Ministerio de las TIC en el marco de la estrategia de TI, denominado Modelo de Seguridad y Privacidad de la Información MSPI.

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Código: M-GT-SGC-200-001
			Versión: 0.0
			Fecha Aprobación: 01/03/2023
			TRD 200-28.11
			Página 5 de 23

GLOSARIO

Acceso a la Información Pública:

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

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).

Amenazas

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

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Autorización

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Datos Personales

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 6 de 23	

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 estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Sensibles

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede 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 la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

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).

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)

Gestión de incidentes de seguridad de la información

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Código: M-GT-SGC-200-001
			Versión: 0.0
			Fecha Aprobación: 01/03/2023
			TRD 200-28.11
			Página 7 de 23

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, art6)

Ley de Habeas Data

Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública

Se refiere a la Ley Estatutaria 1712 de 2014.

Protocolo IPv6

Es la versión 6 del Protocolo de Internet (IP por sus siglas en inglés, Internet Protocol), es el encargado de dirigir y encaminar los paquetes en la red, fue diseñado en los años 70 con el objetivo de interconectar redes; diseñado para reemplazar a Internet Protocolo versión 4 (IPv4) RFC 791, que a 2016 se está implementando en la gran mayoría de dispositivos que acceden a Internet.

Registro Nacional de Bases de Datos

Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

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.

Responsable del Tratamiento de Datos

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).

Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 8 de 23	

Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales

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

Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Partes interesadas (Stakeholders)

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 9 de 23	

OBJETIVOS

OBJETIVO GENERAL

Generar el Modelo de Seguridad y Privacidad de la Información, el cual es el documento que guía la implementación de controles de seguridad y privacidad de la información

OBJETIVOS ESPECÍFICOS

- 1. Dar a conocer la estrategia de seguridad de la información implementada.
- 2. Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- 3. Hacer uso idóneo de los recursos de TICS (Humano, Físico, Financiero, Tecnológico, etc.).
- 4. Asignar roles y responsabilidades para garantizar la seguridad y privacidad de la información.
- 5. Promover el uso de mejores prácticas de seguridad de la información.

ALCANCE

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013 y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea– GEL con el fin de determinar la estrategia de implementación de los controles de seguridad requeridos para las entidades públicas.

MARCO LEGAL

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.

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 10 de 23	

NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

Tabla1. Decretos marco legal

CONOCIMIENTO DE LA INSTITUCIÓN

MISIÓN

Bomberos de Bucaramanga es una entidad pública que presta un servicio esencial, enfocado a la prevención y atención integral del riesgo, capacitación y formación, con personal competente y equipos especializados, para salvaguardar la vida, ambiente y bienes de la comunidad.

VISIÓN

Ser reconocidos en el 2024 a nivel nacional, como la entidad bomberil oportuna y efectiva en la prevención y atención del riesgo y emergencias en el departamento de Santander.

VALORES INSTITUCIONALES

Definimos los valores éticos como aquellos que deben distinguir nuestra entidad y guiar la actuación y desempeño de cada colaborador como persona y miembro de Bomberos de Bucaramanga, estos valores son:

- Compromiso
- Honestidad
- Justicia
- Objetividad
- Participación
- Respeto
- Confidencialidad
- Responsabilidad
- Transparencia
- Lealtad

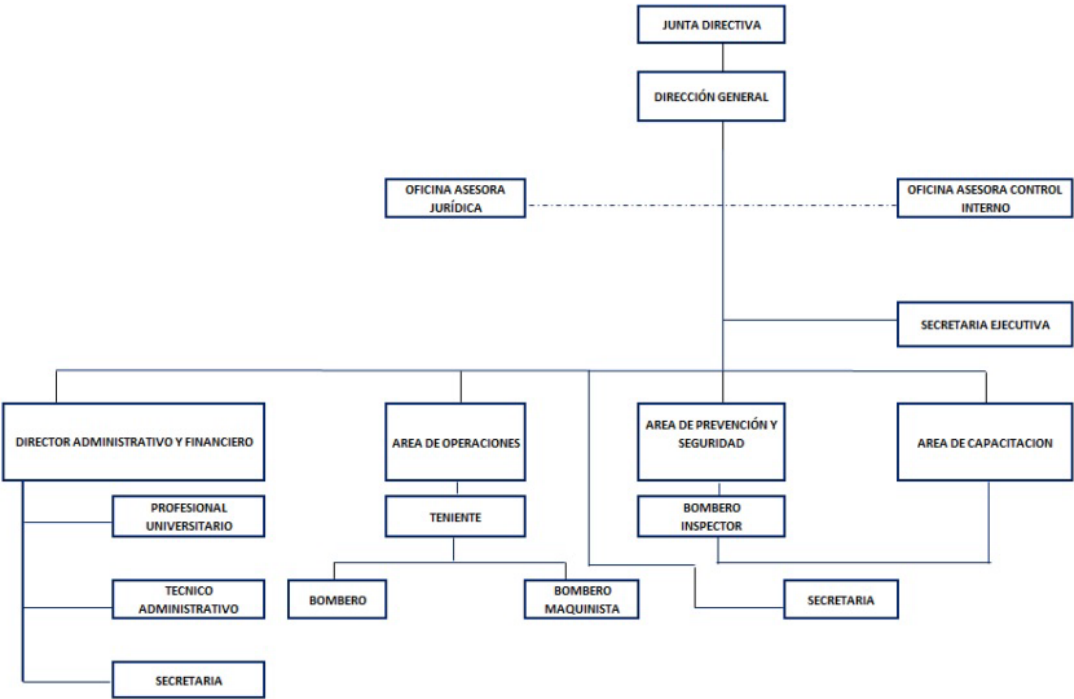
EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 11 de 23	

- Abnegación

ORGANIGRAMA

CUERPO OFICIAL DE BOMBEROS DE BUCARAMANGA



La estructura actual de Bomberos de Bucaramanga fue adoptada mediante Acuerdo Directivo N°. 001 del 12 de Julio de 2006, y ajustada por el Acuerdo Directivo N° 003 del 14 de Diciembre de 2014.

Ilustración 1. Estructura Orgánica

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Basados en el Decreto 2573 de 2014 contenida en el Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la información y las Comunicaciones; el cuerpo oficial de Bomberos de Bucaramanga trabaja constantemente en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la normatividad vigente e implementación de mejores prácticas relacionadas con seguridad de la información.

En efecto, el modelo del SGSI del cuerpo oficial de bomberos de Bucaramanga se encuentra basado en el ciclo de mejoramiento continuo **PHVA (Planear, hacer, verificar y actuar)**, el

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 12 de 23	

cual permite la verificación continua y mejoras efectivas de acuerdo a las necesidades con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.

El modelo de seguridad y privacidad de la información contempla un ciclo de procedimientos que consta de cinco (5) ciclos, que permiten ejecutar adecuadamente la seguridad y privacidad de sus activos de información.

El Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

CICLO PHVA (PLANEAR, HACER, VERIFICAR Y ACTUAR)

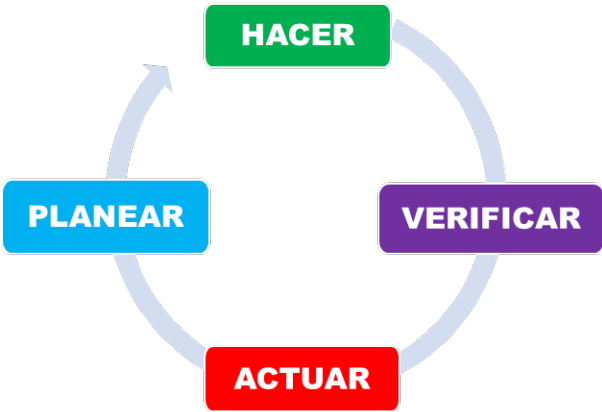


Ilustración 2. Fases del Ciclo PHVA

El ciclo PHVA fue introducido por primera vez por **Walter Shewhart**, el padre del control estadístico de la calidad, **W. Edwards Deming** amplió la idea de Shewhart y utilizó el método científico no solo para el control de la calidad sino también para la mejora de los procesos. Deming se dedicó a enseñar el método a ingenieros japoneses por lo que se mezcló con el método Kaizen (principio japonés de mejora continua, desarrollado por **Kaoru Ishikawa**), para convertirse en lo que hoy llamamos el ciclo **Planificar-Hacer-Verificar-Actuar**.

Planear

Para planear necesitamos definir que necesitamos hacer por lo que se debe tener información precisa como:

- Objetivos del proyecto
- Métricas de éxito
- registro y resultado final del proyecto

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 13 de 23	

- Involucrados en el proyecto
- Cronograma de actividades
- Hallazgos importantes

Cada vez que se ejecuta el ciclo PHVA, evalúa el proyecto para avalar que esté actualizado y sea adecuado para el cumplimiento del proyecto.

Hacer

En esta fase se implementa el plan de proyecto a una mínima escala de forma gradual para verificar el funcionamiento.

Verificar

Comprobar que la prueba en el ciclo hacer se ejecutara de acuerdo a lo programado y si resultan hallazgos se corrigen en la etapa Hacer para que no tengan trascendencia significativa de ser imprescindible, comprobar el programa a seguir para la ejecución del proyecto con el fin de asegurar que se avanza de acuerdo a lo planificado de lo contrario realizar los cambios pertinentes.

Actuar

Consiste en poner en funcionamiento todas las modificaciones del proyecto y los procesos. El PHVA es un ciclo por lo que, si lo requiere, se ejecuta nuevamente y ubicarnos en la fase ‘Planificar’ para realizar mejoras constantemente.

DESCRIPCIÓN CICLO DE OPERACIÓN

Especificación detallada de las etapas del ciclo de funcionamiento del modelo de operación.

EXCELENCIA Y COMPROMISO



Ilustración 3. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Diagnóstico



Ilustración 4. Etapa de Diagnostico del Ciclo de Operación.

En esta etapa se identifica el estado actual del cuerpo oficial de bomberos de Bucaramanga, con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, y para tal efecto se utiliza la herramienta “Instrumento de Evaluación MSPI”, suministrada por el Ministerio de las TIC para efectuar el auto análisis.

- Establecer el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Definir el avance de la implementación del ciclo de operación al interior de la entidad.

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 15 de 23	

- Delimitar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

En esta etapa se tomarán como documentos fuente, los instrumentos suministrados por el Ministerio de las TIC:

- Instrumento de evaluación MPSI
- Instructivo para el diligenciamiento de la herramienta
- Guía No 1 - Metodología de Pruebas de Efectividad

Planificación



Ilustración 5. Etapa de planificación del Ciclo de Operación.

Basados en los resultados de la etapa anterior, se proyecta el plan de seguridad y privacidad de la información alineado al objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, mediante la metodología de gestión del riesgo.

- Fijar el alcance del sistema.
- Plantear la metodología de riesgos.
- Definir el plan de tratamiento de riesgos.

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 16 de 23	

- Establecer políticas de seguridad de la información. Manual aprobado por el comité y la alta dirección con las políticas de seguridad y privacidad de la información.
- Inventario de activos de información. Documento con metodología para identificación, valoración, de activos de información.
- Integración MSPI, con el sistema de gestión documental del cuerpo oficial de bomberos de Bucaramanga.
- Documentación del plan diagnóstico para la transición Ipv4 a Ipv6

Para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

Implementación



Ilustración 6. Etapa de Implementación del Ciclo de Operación.

El cuerpo oficial de Bomberos de Bucaramanga, debe programar, aplicar y dirigir los procedimientos indispensables para ejecutar con los requisitos de seguridad y privacidad de la información que permitan llevar a cabo las actividades indicadas en el plan de tratamiento de riesgos.

Se debe registrar cada proceso ejecutado según lo programado con el fin de controlar los cambios a ejecutar y permitir tomar acciones que aminoren los efectos adversos cuando sea indispensable.

Designar el encargado de seguridad de la información a través del comité de gestión institucional aprobado por la alta dirección.

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 17 de 23	

Documento detallado con estrategias del plan de implementación de IPv6 y guía de aseguramiento del protocolo IPv6 aprobado por la oficina de Tics de la entidad.

Evaluación de desempeño

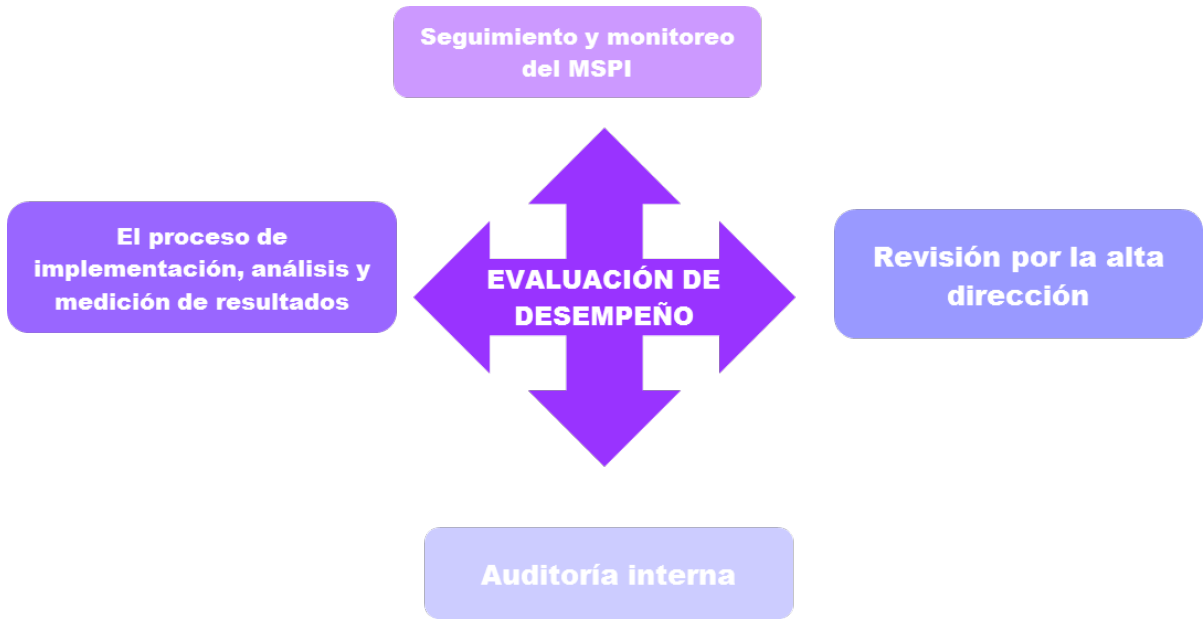


Ilustración 7. Etapa de evaluación de desempeño del Ciclo de Operación.

El proceso de monitoreo, análisis, medición de resultados, seguimiento y monitoreo del MSPI se realiza a partir de los resultados que contienen los indicadores de seguridad de la información proporcionados para verificación del proyecto implementado.

La ejecución del plan de actividades que permiten demostrar la eficiencia del MSPI contiene:

- Evaluación de la eficiencia de los parámetros establecidos y el cumplimiento de los objetivos de seguridad.
- Comprobación de la ejecución de los niveles de riesgo
- Seguimiento a la implementación de las actividades de ejecución alcance del MSPI.
- Evaluación de los indicadores de gestión del MSPI

Ejecución de auditorias

Se realiza un documento de programación de auditorías para el MSPI en el que se debe registrar la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. La ejecución de las auditorias y revisiones se deben realizar con los requisitos programados y es importante realizar algunas exprés con el fin de garantizar e identificar las falencias y aciertos reales, con el fin de que los hallazgos sean lo más precisos posibles y así garantizar la corrección eficiente y dar cumplimiento con todos los requerimientos.

MEJORA CONTINUA



Ilustración 8. Etapa de mejora continua del Ciclo de Operación.

En esta fase se especifica y ejecuta el programa de mejoramiento continuo con base en los resultados de la fase de verificación.

De los resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI se procede a realizar los ajustes necesarios para corregir los hallazgos de las auditorias, el cuerpo oficial de bomberos de Bucaramanga

En los documentos entregables se realizan los ajustes, controles y procedimientos dentro del MSPI.

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 19 de 23	

El resultado nos arroja el plan de mejoramiento y comunicación continua revisada y aprobada por la alta dirección de la entidad, la que especifica las decisiones, variaciones, prioridades aprobadas en los comités.

MODELO DE MADUREZ

Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentran la Entidad, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado. Es decir, se aplica en la fase de Diagnóstico y como herramienta de evaluación de los avances de la implementación del modelo

En el ámbito de la Seguridad de la información, los componentes del sistema se ubican en diferentes niveles de acuerdo a su importancia, a continuación, se ilustran dichos componentes:

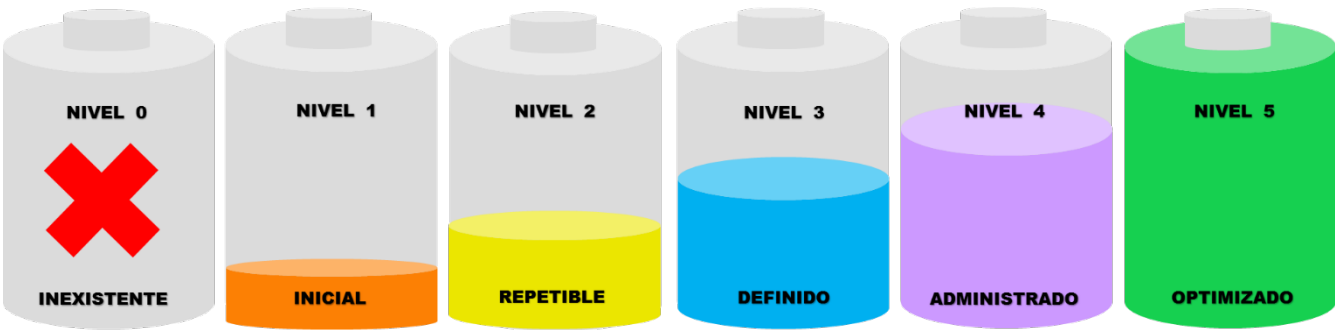


Ilustración 9. Modelo de madurez

Inexistente

No implementa la seguridad de la información.
No contempla la importancia de la seguridad de la información, por lo que no se reconoce como un activo indispensable para la misión y objetivos estratégicos

Inicial

Tiene problemas de seguridad de la información que deben ser resueltos, por lo que se identifican las falencias se determina la implementación del MSPI, creando políticas, procesos y procedimientos que den soluciones a las amenazas de seguridad de la información

Repetible

Tiene procesos informales de seguridad. Se determina y clasifican los activos de información. Se sensibiliza los servidores públicos en el tema de seguridad y privacidad de la información.

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 20 de 23	

Se establece el diagnóstico de migración a Ipv6

Definido

Se ha ejecutado el diagnóstico donde se evidencia el estado de la entidad, se determinaron los objetivos, alcance, límites y políticas de seguridad de la información

Se asignaron roles responsabilidades y metodología para el tratamiento de seguridad y privacidad de la información.

Se implementa plan de tratamiento de riesgos y se dispone el proyecto de transición de Ipv4 a IPV6

Administrado

Se ejecuta la fase de desempeño y mejora continua.

Se inspecciona y da seguimiento periódicamente a los activos de información del cuerpo de bomberos de Bucaramanga.

Se califica el cumplimiento de las políticas de seguridad y privacidad de la información.

Se mide la efectividad de los controles para disminuir los incidentes y prevenirlos en el futuro.

Se crean un entorno de prueba para el uso del protocolo IPv6.

timizado

Se implementa la seguridad de la información como valor agregado.

Hay efectividad en el cumplimiento de los objetivos misionales

La entidad tiene uso pleno en IPV6.

El nivel de madurez del MSPI, busca determinar la condición actual de seguridad de la información en las entidades del estado.

ADOPCIÓN DEL PROTOCOLO IPv6

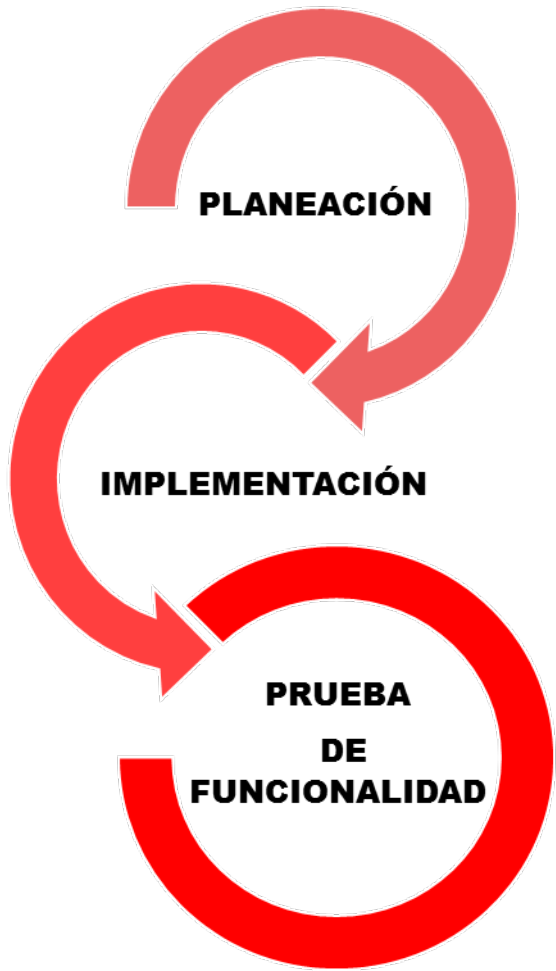


Ilustración 10. Modelo de madurez

Se concreta el proyecto estratégico de transición de IPv4 a IPv6 para garantizar la ejecución adecuada de adaptación y dar cumplimiento a la implementación del nuevo protocolo.

PLANEACIÓN

- Se hace levantamiento del inventario hardware y software
- Informe de la infraestructura de la red de comunicaciones
- Indicaciones para la adquisición de equipos de cómputo que sean compatibles con IPv6
- Documento con estrategia de implementación y aseguramiento del protocolo IP

IMPLEMENTACIÓN

Realizar prueba piloto realizando montaje, ejecución y corrección de configuraciones del direccionamiento IPv6, activar las políticas de seguridad de IPv6, comprobar la funcionalidad de los servicios y aplicaciones del cuerpo de Bomberos de Bucaramanga.

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 22 de 23	

Registro de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

Basarse en las Guía No 20 – Guía Transición de IPv4 a IPv6 para Colombia, Guía No 19 - Guía de Aseguramiento del Protocolo IPv6 para el proceso de migración.

PRUEBAS DE FUNCIONALIDAD

Realizar pruebas de funcionalidad y/o monitoreo de IPv6, en sistemas de información, de almacenamiento, de comunicaciones y servicios; frente a las políticas de seguridad perimetral, de servidores de cómputo, equipos de comunicaciones, de almacenamiento, entre otros.

Elaborar un inventario de servicios y sistemas de información que trabajen con los parámetros del protocolo IPv6.

Crear registro detallado de los cambios las configuraciones realizadas, previo al análisis de funcionamiento realizado en la etapa de Implementación.

Acta de cumplimiento a satisfacción del cuerpo oficial de Bomberos de Bucaramanga con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la etapa de implementación.

Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.

FIRMAS Y REVISIONES

TITULO	MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CUERPO OFICIAL DE BOMBEROS DE BUCARAMANGA	
AUTOR	Oficina de Sistemas e Informática - OSI	
TEMA	Seguridad y Privacidad de la Información	
FECHA DE ELABORACIÓN	Diciembre del 2022	
FORMATO	PDF	
VERSIÓN	1.0	
PALABRAS RE-LACIONADAS	Información, Sistema de Gestión de Seguridad de la Información – SGSI, Modelo de Seguridad y Privacidad de la Información – MSPI, Plan Estratégico de Tecnologías de Información y Comunicación – PETI, Políticas, Confidencialidad, Integridad, Disponibilidad y Privacidad.	

EXCELENCIA Y COMPROMISO

	MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: M-GT-SGC-200-001	
		Versión: 0.0	
		Fecha Aprobación: 01/03/2023	
		TRD	200-28.11
		Página 23 de 23	

CONTROL DE CAMBIOS

NOMBRE	VERSIÓN	AUTOR	FECHA
MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CUERPO OFICIAL DE BOMBEROS DE BUCARAMANGA	0.0	Oficina de Sistemas de Informática - OSI	01 marzo 2023