BOMBEROS DE BUCARAMANGA

PETI - PLAN ESTRATÉGICO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN VIGENCIA 2022

PL-GT-SGC-110-005

Alcaldía de Bucaramanga

GOBERNAR ES HACER

1. OBJETIVO GENERAL

El objetivo general del Plan Estratégico de tecnologías de la información – PETI de Bomberos de Bucaramanga, tiene como finalidad establecer las estrategias para el diagnóstico, análisis, y planeación de los proyectos de tecnología de la información y las comunicaciones durante los años 2020 - 2023, alineado con los objetivos y metas institucionales.

1.1 Objetivos Específicos

Para la oficina TIC de Bomberos de Bucaramanga sus objetivos estratégicos son los relacionados a continuación:

- Revisar y actualizar los procesos de Bomberos de Bucaramanga que en la actualidad se realizan de manera operativa y automatizarlos.
- Actualizar y Renovar la Plataforma Tecnológica (PT) de Bomberos de Bucaramanga.
- Actualizar y Mantener en operación los aplicativos y sistemas de información propios y licenciados que soportan los procesos misionales de la entidad.
- Brindar soporte a los macro procesos estratégicos establecidos en el mapa de procesos de la entidad.

2. ALCANCE

El presente documento se elabora con la intención de definir el marco de acción estratégica de BOMBEROS DE BUCARAMANGA en el área de Tecnología de Información para el periodo 2020-2023.

3. RESPONSABLE

Dirección General y Dirección Administrativa y financiera

4. GLOSARIO

Activo: Cualquier cosa que tiene valor para la organización.

Amenaza: Es un riesgo alto al que pueden estar expuestas las organizaciones, los cuales pueden afectar sus activos con pérdidas irrecuperables en sus datos, equipos o infraestructura.

Antivirus: Es un sistema informático que se encarga de detectar y eliminar los virus que pueden dañar información importante para la organización.

Ataque: Debilidad o falla, que es aprovechada por uno más individuos para dañar un sistema de información.

Backup: copias de seguridad que se realizan a todos los equipos de la entidad, incluyendo servidores, en diferentes medios de almacenamiento.

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

Contraseña: Secuencia secreta de caracteres numéricos o alfanuméricos permitiendo el acceso a un usuario a un equipo, un archivo o sistema de información.

Disponibilidad: Asegurar que la información esté disponible.

Emergencias: Situación de peligro o desastre, que puede derivar perdida de personas y/o enseres.

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

Gobierno Digital: Su objetivo primordial es aprovechar el uso de las tecnologías de la información y de comunicaciones en aras del funcionamiento de las entidades públicas con el fin de agilizar la tramitología a los ciudadanos y realizarlo de manera transparente.

Página web: Documento de tipo electrónico, que contiene información digital, capaz de contener datos visuales y/o sonoros o una mezcla de ambos, a través de textos, imágenes, gráficos, audio o vídeos y otros tantos materiales dinámicos o estáticos.

Prevención: Es una medida o disposición que se debe tomar con anterioridad para evitar que se materialice una cosa considerada negativa.

Política de Seguridad: Es un conjunto de documentos, reglas o procedimientos que deben implementarse para mantener y resguardar la seguridad de la información.

Redes Sociales: Son aplicaciones web que son utilizadas por los usuarios para interactuar temas familiares, personales, o laborales.

Riesgo Informático: El riesgo informático se define como “la probabilidad de que una amenaza en particular expone a una vulnerabilidad que podría afectar a la organización”, o como “la posibilidad de que algo pueda dañar, destruir o revelar datos u otros recursos.

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.

Servicio: Conjunto de actividades, que apoyan los procesos de una entidad para responder a las necesidades de los usuarios.

Software: Programas fuente, programas objeto, utileras, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Soporte Técnico: Es un rango de servicios por medio del cual se proporciona asistencia a los usuarios al tener algún problema al utilizar un producto o servicio, ya sea este el hardware o software de una computadora de un servidor de Internet, periféricos, artículos electrónicos, maquinaria, o cualquier otro equipo que este dentro de los activos de una organización.

Usuario: Persona que utiliza un sistema informático, incluyendo equipos de cómputo, equipos de impresión, o sistemas de información.

Vulnerabilidad: La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

5. CONDICIONES GENERALES

La dirección general y Administrativa en conjunto con el apoyo de telemática continuara monitoreando la ejecución de cada una de las necesidades y procesos del área que administra los diferentes sistemas de información para dar cumplimiento a los lineamientos a la política de Gobierno Digital.

La dirección general y Administrativa en conjunto con el apoyo de telemática continuara dando cumplimiento a cada una de las estrategias de las tecnologías de la información propuestas teniendo en cuenta su importancia y el presupuesto disponible para tal fin.

6. DOCUMENTOS DE REFERENCIA

Guía para la construcción del PETI

Guía cómo estructurar el Plan Estratégico de Tecnologías de la información – PETI

Modelo PETI – MINTIC

7. MARCO LEGAL

Los siguientes documentos de referencia, normativos, vinculantes hacen parte integral del presente documento, sus consideraciones, alcance y construcción

1. Plan de Desarrollo Municipal, Alcaldía de Bucaramanga 2020 -2023
2. Decreto 415 de 2016. Artículo 2.2.35.3 (lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones)
3. G.ES.06 Guía Estructura PETI (MinTIC)
4. Marco Jurídico Institucional de la Estrategia - Decreto Único Sectorial 1078 de 2015
5. Conpes 3650 (Gobierno en línea)
6. Conpes 3785 (Servicios al ciudadano)
7. Ley 1345/2009 (Marco Sector TIC)
8. Decreto 2482 de 2012 (Anti trámites)
9. Gobierno Digital
10. Decreto 1078 de 2015 del Sector TIC - Título 9 - Capítulo 1 (Mapa de ruta de excelencia estrategia Gobierno Digital).

8. DESARROLLO

8.1 Elementos Declarados en la Misión

Presta sus servicios de Prevención, Seguridad, y Atención Integral del Riesgo en la comunidad de Bucaramanga y donde los compromisos Institucionales lo requieran a nivel nacional o internacional sin distingos de ninguna índole.

- Atender emergencias en el Municipio de Bucaramanga.
- Prestar apoyo en atención de emergencias a otros municipios cuando se presente la necesidad.
- Prestar servicios de prevención.
- Atender integralmente riesgos de la comunidad.
- Atender incidentes con materiales peligrosos.
- Realizar inspecciones de Prevención de riesgos a establecimientos públicos, comerciales e industriales.
- Realizar revisión técnica de seguridad humana en edificaciones particularmente en establecimientos públicos, industriales y comerciales.
- Realizar revisión técnica de seguridad humana para el acompañamiento de eventos masivos y/o pirotécnicos de acuerdo con la normatividad vigente en cuanto a gestión integral del riesgo contra incendio.
- Revisar los diseños de los sistemas de Protección contra incendio y seguridad humana de los proyectos de construcciones y/o reformas de acuerdo con la Ley Bomberil (1575 de 2012) y Resolución 0661 del 26 de Junio de 2014.
- Atender siniestros y calamidades públicas.
- Capacitar en Brigadas de emergencia según solicitudes de las empresas comerciales e industriales del área metropolitana.
- Gestionar ante las instituciones competentes la capacitación, entrenamiento y formación Bomberil para el personal operativo de la entidad.

Desde el origen de la MISIÓN, el área de TI en la entidad adquiere un rol de apoyo en los sistemas de Información y de comunicación que son fundamentales en la prestación y cobertura del servicio esencial.

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

Dentro de la Visión de la entidad se destaca las declaraciones:

- Institución Bomberil comprometida con la comunidad, en la objetiva gestión integral del riesgo, garantizando los recursos necesarios para alcanzar estándares internacionales.

- Lograr la excelencia en el servicio.

Este es un aspecto que desde la perspectiva se cuentan con recursos humanos, tiempo y espacio los que requieren de un aprovechamiento y un entrenamiento al máximo, puesto que son declaraciones de un compromiso con la comunidad, para llegar a la excelencia en la prestación del servicio, siendo este, el de preservar la vida y los bienes de la comunidad, por tal razón sus expectativas de ser protegidos y salvados en el momento de una emergencia son determinantes para que la visión pueda ser cumplida.

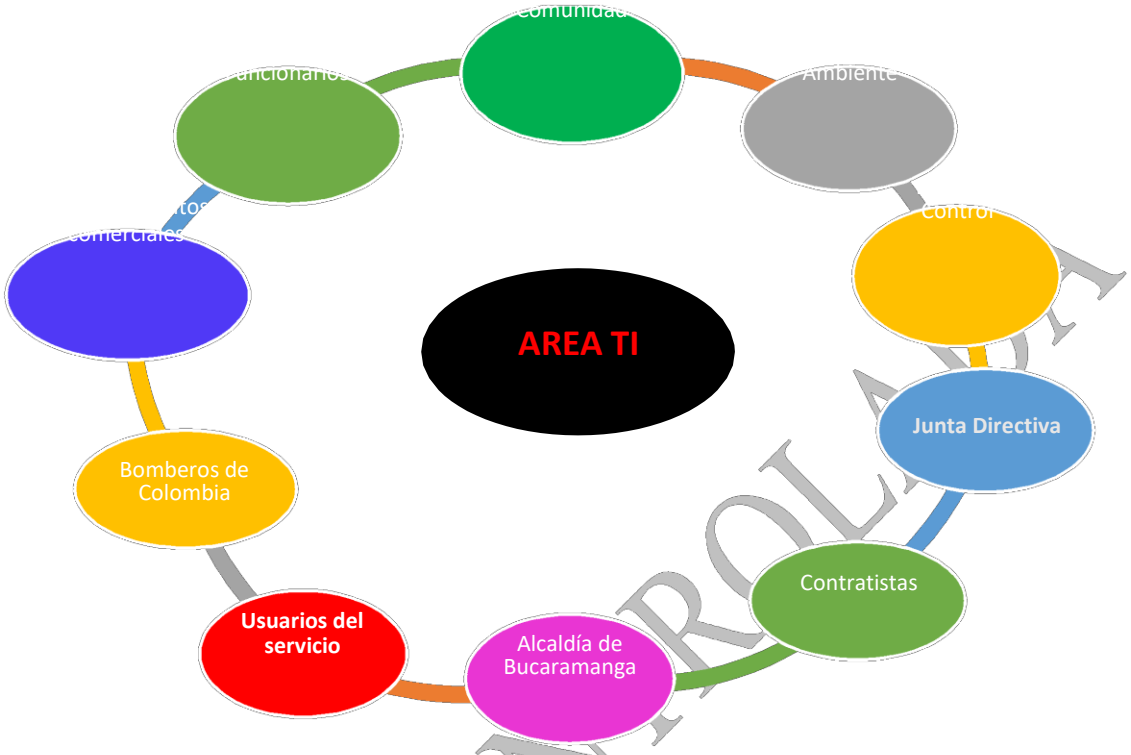
Para el cumplimiento de la Visión a 2.022, de acuerdo con los elementos incorporados está el recurso tiempo, lo cual no solamente se refiere al tiempo en llegar a ser reconocidos sino el tiempo en llegar a la excelencia, que significa el logro exitoso en los eventos que intervenga la entidad.

MISIÓN

Bomberos de Bucaramanga, es una Institución 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.

En ejercicio de su autonomía, trabaja para la comunidad en la gestión integral del riesgo contra incendio, los preparativos y atención de rescates en todas sus modalidades, la atención de incidentes con materiales peligrosos y la realización de las labores de inspección y revisión técnica en prevención de incendios y seguridad humana, interviniendo oportunamente para salvaguardar la vida y bienes de la comunidad, entre otras. Por lo anterior, la Entidad cuenta con personal capacitado, con equipos y maquinaria especializados.

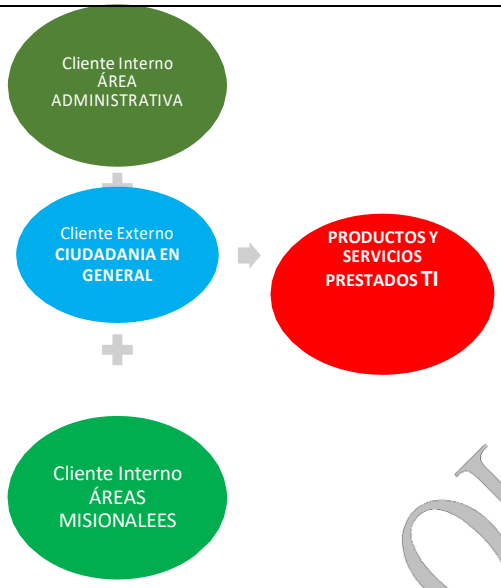
8.2 Stakeholders (Partes Interesadas)



Gráfica No. 1

Los Stakeholders que se atienden en función de los sistemas de información y tecnología de comunicaciones de Bomberos de Bucaramanga tienen acceso a la prestación del servicio mediante diferentes mecanismos tanto virtuales como de forma personalizada.

8.2.1 Usuarios de Bomberos de Bucaramanga



Gráfica No. 2 Usuarios de Bomberos de Bucaramanga

El área TI de Bomberos de Bucaramanga atiende, presta servicios de helpdesk y apoyo en la operación mediante programas y herramientas tecnológicas a tres clientes como son el 1. Área administrativa que la componen todas las áreas de la entidad, 2. Área Operaciones de la entidad prestando apoyo en la prestación del servicio mediante las herramientas tecnológicas en comunicaciones, programa Sistema de Gestión Bomberos y la ciudadanía en general del Municipio de Bucaramanga que está identificada entre ciudadanos, áreas urbana y rural a quienes presta el servicio de la gestión integral del riesgo contra incendio, los preparativos y atención de rescates en todas sus modalidades y la atención de prevención y atención de desastres (La gestión integral del riesgo contra incendio, los preparativos y atención de rescates en todas sus modalidades y la atención de incidentes con materiales peligrosos es responsabilidad de todas las autoridades y de los habitantes del territorio colombiano, en especial, los municipios, o quien haga sus veces, los departamentos y la Nación)

8.2.2 Gobierno Digital

El líder de la política de gobierno Digital es el Ministerio de las tecnologías de información y comunicación quien a través de la dirección de Gobierno Digital se encarga de emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de Política Digital, en las entidades Públicas del orden Nacional y Territorial. El responsable institucional de la política de Gobierno Digital es el Representante Legal de cada sujeto obligado y es el responsable de coordinar, hacer seguimiento y verificación de la implementación de la política de Gobierno Digital.

El responsable de orientar la implementación de la política de Gobierno Digital: es el comité institucional de Gestión y desempeño de que trata el Decreto 1083 de 2015; conforme a lo establecido en el modelo integrado de planeación y gestión (MI PG). Teniendo en cuenta que el nuevo enfoque de Gobierno Digital es el uso de la tecnología

como una herramienta que habilita la gestión de la entidad para la generación de valor público, todas las áreas o dependencias son corresponsables en la implementación.

Para Bomberos de Bucaramanga a partir de la elaboración del PETI se requiere adoptar e implementar los lineamientos de la Política de Gobierno Digital a partir de enero de 2019.

8.2.3 Propósito

- El alcance del Plan Estratégico de Tecnología de la Información es la de adoptar una plataforma para el período 2020-2023, el cual pretende para el último año, el desarrollo tecnológico e innovador, eficiente y efectivo que pueda contribuir de manera significativa en la implementación de una plataforma tecnológica para la entidad. Así mismo, que pueda contar con un sistema de información propio.

- Es importante señalar que se debe mantener un plan de comunicación interrelacionado con las Tecnologías de la Información y desarrollo de la Estrategia Nacional de Gobierno Digital.

- Dentro de la estrategia de comunicación y las tecnologías de la información es importante para la entidad la adquisición de un sistema de información propio para la operatividad misional.

- Diseñar e implementar un plan estratégico de tecnologías de la información para la entidad, que permita mediante actividades administrativas, técnicas y tecnológicas; la planificación, el manejo y organización de la documentación e información soportada en los diferentes medios de almacenamiento producida y recibida desde su origen hasta su disposición final con el fin de facilitar su confidencialidad, disponibilidad e integridad.

8.2.4 Situación Actual

Actualmente Bomberos de Bucaramanga, como entidad cuenta con una persona al frente de los requerimientos de TI. No hay un plan previamente establecido de TI en cuanto al avance o crecimiento de la entidad y sus estrategias operacionales y administrativas.

La persona que apoya los procesos de los requerimientos de TI de Bomberos de Bucaramanga. Atiende solamente al cliente interno en sus necesidades soporte, configuración, mantenimiento, copias de seguridad, capacitación y continuidad de los sistemas de información, equipos, y apoyo a los diferentes procesos del área administrativa de la Entidad.

Bomberos de Bucaramanga, requiere El Plan Estratégico de Tecnologías de la Información y las Comunicaciones, con el fin de modernizar el uso de las tecnologías de la información y las comunicaciones (TIC), de manera organizada, planificada, haciendo uso eficiente de los recursos para el desarrollo del objetivo Institucional.

A la fecha la entidad cuenta con una Política de Seguridad y Privacidad de la Información implementada pero no se está aplicando en todas las áreas, esta desinformación acarrea a que no se pueda contribuir a salvaguardar la información, y no se minimiza el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información.

8.2.5 Estrategia TI o modelo empresarial en curso

Actualmente no existe una estrategia de TI establecida por la entidad que apoye el desarrollo de la misión de manera sostenida; sin embargo, cuenta con Sistemas de Información que fortalecen la prestación del servicio en las áreas misionales; las cuales que constan de cinco (5) módulos que operan de forma articulada y generan información de la prestación del servicio; como por ejemplo, podemos mencionar entre otros las certificaciones de atención de emergencias, inspecciones a establecimientos, certificaciones para la realización de eventos masivos y/o pirotécnicos y capacitaciones realizadas tanto en formación Bomberil como en capacitaciones en Prevención a Establecimientos públicos y privados.

8.3 Atención a la Ciudadanía

Bomberos de Bucaramanga para la atención al ciudadano tiene dispuesto varios mecanismos de atención como son: Atención personalizada, página web, virtual.

Como mejora se habilitó el módulo PQRS en la Página WEB para garantizar el registro y trazabilidad de las peticiones, quejas y reclamos ingresadas por este medio, el cual requiere para su funcionamiento la inducción del personal asignado para su manejo, el monitoreo y la administración del módulo.

Adicionalmente se cuenta con un espacio físico para la atención al ciudadano de manera presencial y se avanza en el rediseño del procedimiento para atención de PQRSD ajustado a los cambios en el marco normativo como Estatuto Anticorrupción, Ley anti- trámites, y Ley 1712 de 2014, Ley Transparencia de la Información.
Existen varios canales de atención que Bomberos de Bucaramanga, pone a disposición de la ciudadanía para el acceso a los trámites, servicios y/o información de la entidad, así:

- ✓ Presencial: Ventanilla única
- ✓ Telefónica: línea de emergencias 119
- ✓ Línea Fija o conmutador: 6526666
- ✓ Virtual: Chat, correo electrónico,
- ✓ Escrito: Radicación de correspondencia
- ✓ Buzón de Sugerencias ubicado en el primer piso.

8.4 Gobierno Digital

El líder de la política de gobierno Digital es el Ministerio de las tecnologías de información y comunicación quien a través de la dirección de Gobierno Digital se encarga de emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la Política Digital, en las entidades Públicas del orden Nacional y

Territorial. El responsable institucional de la política de Gobierno Digital es el Representante Legal de cada sujeto obligado y es el responsable de coordinar, hacer seguimiento y verificación de la implementación de la política de Gobierno Digital.

El responsable de orientar la implementación de la política de Gobierno Digital: es el Comité Institucional de Gestión y desempeño de que trata el Decreto 1083 de 2015; conforme a lo establecido en el modelo integrado de planeación y gestión (MI PG).

Teniendo en cuenta que el nuevo enfoque de Gobierno Digital es el uso de la tecnología como una herramienta que habilita la gestión de la entidad para la generación de valor público, todas las áreas o dependencias son corresponsables en la implementación.

Gobierno Digital es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC, que tiene como objetivo "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".
El Ministerio de las tecnologías de la información y las comunicaciones MINTIC a través de la dirección de Gobierno Digital presentó la política expresada en el Decreto 1008 del 14 de junio de 2018. Cuyo objetivo es incentivar el uso y aprovechamiento de las TIC para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.
De esta manera, la entidad busca, no solo que el uso de la tecnología sea ágil, sencilla y útil para las personas, sino también que la interacción entre los actores involucrados en la política se de en un ambiente seguro y previsible y en nuestro caso forme parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores. El Manual de Gobierno Digital será la guía para la formulación del Plan estratégico de las tecnologías de la información PETI para Bomberos de Bucaramanga que orientará la ruta de acción que deben seguir las entidades públicas para adoptar la política.

Bomberos de Bucaramanga, adopta la Política Digital emanada del Ministerio de las TIC, como política Digital para ser implementada en la entidad como parte de Gobierno Digital.

8.5 Inventario de Software y Aplicativos

En relación a lo anterior, se puede clasificar las versiones de sistemas operativos de la siguiente manera:

SISTEMAS OPERATIVOS
Microsoft Windows 7 64 bits
Microsoft Windows 8 64 bits
Microsoft Windows 10 64 bits

Windows Server 2012 R2 Standard
Windows Server 2016 R2 Standard
Sophos Firewall

Tabla No. 1 sistemas operativos

En cuanto a suites de ofimática, se trabaja con herramientas de Microsoft tales como: Microsoft Office 2013, 2016 y 2019. Adicionalmente, se cuenta con la solución de Antivirus Kaspersky Advanced la cual se administra desde una consola en el servidor y satisface las necesidades de los usuarios.

De igual manera a nivel de servidores se cuenta con licencias para motores de bases de datos de SQL Server y Postgres en los cuales se centraliza la mayor carga de procesamiento de transacciones para los procesos misionales y administrativos de Bomberos de Bucaramanga tales como contabilidad, nómina, inventarios, facturación y presupuesto.

8.6 Sistema Telefónico

Actualmente contamos con 29 extensiones telefónicas IP´s en funcionamiento, de las cuatro (4) líneas análogas solo se están utilizando dos (2) líneas, se ha tenido inconvenientes de intercomunicación interna y externa con la línea del área de Inspectores y se soluciona con el soporte de Movistar

De las líneas análogas existe un cableado para la red de voz sin etiquetado y esto dificulta un mantenimiento preventivo y correctivo en la red telefónica.

TELEFONOS IP
141
137
136
135
134
133
132
130
129
127
126
123
122
121
117
116
115
114
113
112

TELEFONOS ANALOGOS
120
131
125
118
4

111
1105
110
109
107
106
104
103
101
29

Tabla 2 extensiones telefónicas

8.7 Red de Datos

Bomberos de Bucaramanga tiene una conexión a internet en su sede principal está contratada con el ISP MOVISTAR, de 100 MB fibra reusó (1:2).

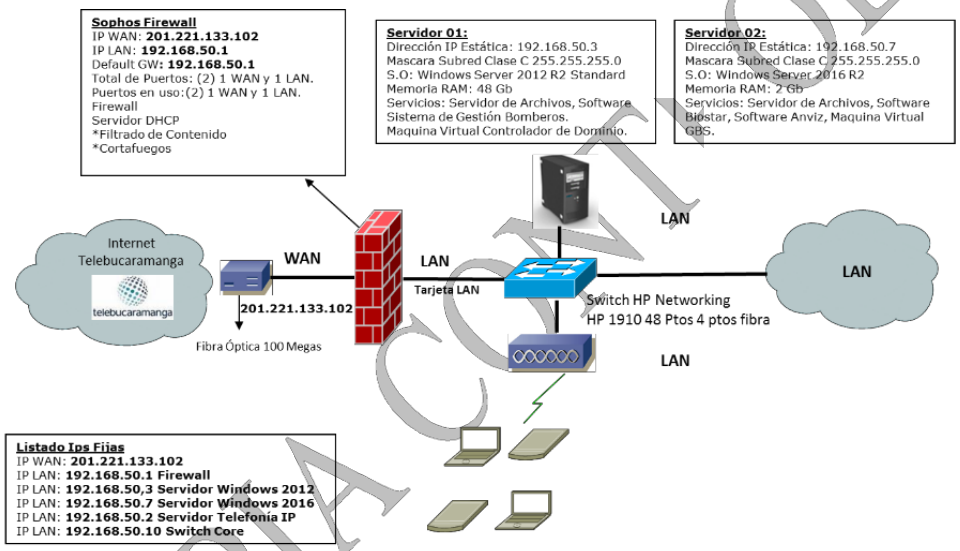


Figura 1 Red de Datos

En el esquema anterior podemos observar la topología actual de la red datos existentes en Bomberos de Bucaramanga para la Estación central.

Igualmente se cuenta con servicios de internet para las sedes de Provenza, chimita, y mutualidad, contratadas con ISP TELEBUCARAMANGA (MOVISTAR), de 8 MB fibra reusó (1:2) para cada sede respectivamente.

Figura 2. Topología Bomberos Bucaramanga – Estación Mutualidad.

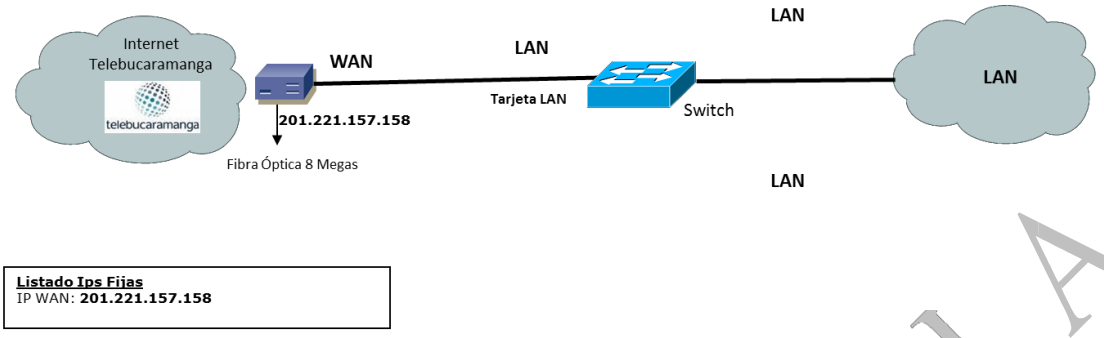
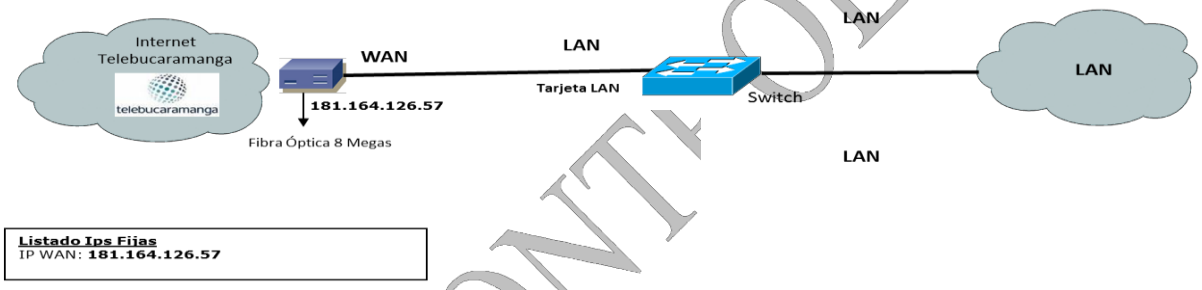


Figura 3. Topología Bomberos Bucaramanga – Estación Chimita



8.8 Plataforma Tecnológica de Bomberos de Bucaramanga.

Actualmente Bomberos de Bucaramanga dispone de una plataforma tecnológica compuesta por un rack de comunicaciones que resguarda los servidores para los servicios corporativos de la Entidad.

Esta plataforma en su infraestructura cuenta con 45 equipos computacionales, y sistemas de almacenamiento compuesto por servidores y de información interconectados que soportan los procesos administrativos y misionales en las diferentes dependencias de la entidad.

Bomberos de Bucaramanga presentó en el año 2017 y 2021, una mejoría en su infraestructura tecnológica consistente en una renovación parcial de un 70% en equipos de cómputo. Se tiene proyectado continuar con este proceso de renovación con el fin de fortalecer los procesos misionales y administrativos que estén relacionados con la prestación del servicio a sus usuarios. Con respecto al mejoramiento en los softwares de entidad; está en proceso la adquisición de dos sistemas para cubrir el área operativa y administrativa establecidos como proyectos de inversión contemplados en el plan de compras para el fortalecimiento institucional que pretende mejorar los procesos de la entidad.

En el marco de la estrategia de Gobierno Digital, se realizó un rediseño en la página web institucional que comprende. 1. Se creó el botón de pagos en línea que propende por el

acceso fácil y seguro de los usuarios en el momento de realizar sus pagos a la entidad por la prestación de su servicio; este mejoramiento contribuye en el cumplimiento para la ley anti tramites.

Así mismo se realizó en el año 2021 la contratación de servicios profesionales para el rediseño, actualización, creación de contenidos, mantenimiento, seguridad e implementación de nuevas funcionalidades para mejorar el rendimiento y operatividad de la página web de Bomberos de Bucaramanga de conformidad a la ley 1712 de 2014, y anexo técnico No. 2 Resolución 1519 de 2020.

8.9 Equipos de cómputo a cargo del área de TI

A continuación, se relaciona el inventario resumen de los equipos de cómputo a cargo del área TI de Bomberos de Bucaramanga:

No.	DESCRIPCION	CANTIDAD	ESTADO	AREA - UBICACIÓN
1	Portatil Dell, Intel core i7 6600, Memoria Ram 8GB, 2.8 GHz	1	Nuevo	Oficina de Control Interno
2	Computador Lenovo, Intel Core i7, Memoria Ram 8GB, CPU 3.41 GHz	11	Nuevo	Dirección administrativa y financiera, secretaria dirección, Juridica, Prevención y seguridad, operaciones, tenientes, inspectores, Recepción documental.
3	Computador HP, Intel core i7, Memoria Ram 4 GB, CPU 3.40 GHz.	1	Bueno	Apoyo Talento Humano
4	Computador todo en uno, Intel core i5, Memoria Ram 4 GB, CPU 2.90 GHz	3	Bueno	Apoyo Capacitaciones. Seguridad y salud, apoyo jurídico
5	Computador HP, Intel core i5, Memoria Ram 4 GB, CPU 5.20 GHz	1	Bueno	Control Interno
6	Computador Intel Core E7500, Memoria Ram 4 GB, CPU 2.93 GHz.	3	Regular	Oficina Jurídica-apoyo, Apoyo Almacén-Contable
7	Portátil Intel Core i7, Memoria Ram 8 GB, 2.30 GHz.	1	Nuevo	Capacitaciones

8	Computador Pentium Dual Core E5200, 2 GB, CPU 2.50 GHz	1	Regular	Apoyo Inspecciones
9	Computador Intel Core i7, 4 GB, CPU 3.40 GHz.	4	Bueno	Administrativo y Financiero, sistemas, Guardia Central, operaciones
10	Computador Intel Core i5, 4 GB, CPU 2.80 Ghz	2	Bueno	Portería y Dirección General
11	Computador Intel Core i7, 8 GB, CPU 3.40Ghz	1	Bueno	Nomina
12	Computador HP ProDesk 400 G7 Intel Core I5-10500, CPU 3.10 Ghz, Ram 32 GB	16	Nuevo	Equipos para cubrir todas las áreas de la entidad y estaciones
13	Portail HP ProBook 455 G7 AMD Ryzen 3 4300U 2.70 Ghz, 16 GB Ram	1	Nuevo	Asesores Juridica

Tabla 3 inventario de Equipos

Dentro de los procesos de transformación digital de las entidades públicas, se recomienda la creación de algunas instancias técnicas, para definir y tomar decisiones operativas y técnicas con relación a la arquitectura empresarial de la entidad. Estas instancias deben actuar en coordinación con el Comité Institucional de Gestión y Desempeño para la toma de decisiones. Entre estas se encuentran:

Grupo de trabajo de Arquitectura empresarial: Este grupo actúa como un comité Técnico de arquitectura empresarial, evalúa los impactos de cualquier decisión de inversión, adquisición o modernización de sistemas de información e infraestructura tecnológica en la entidad. Así mismo, tiene funciones de gobierno.

8.10 Módulos que comprenden el sistema de información

No.	MÓDULO SISTEMA DE INFORMACIÓN	ACTIVIDADES
1	**Sistema de Gestión Bomberos de Bucaramanga CALL CENTER**	Sistema WEB que permite: 1. Registrar las emergencias relacionadas con incendios. Registrar tiempos de atención, 2. Registrar el ingreso y salida del personal, 3. Registra ingreso del vehículo, y 4. Control de los datos registrados en el sitio del incidente.
2	**Sistema de Gestión Bomberos de Bucaramanga Tenientes**	El Sistema de gestión Bomberos de Bucaramanga tenientes, es un servicio, caracterizado por la atención personalizada, atiende y apoya en forma permanente los requerimientos de la comunidad con criterios de eficiencia y eficacia, basados en la continua modernización tecnológica y organizacional y en el desarrollo integral de nuestros servidores.
3		El Sistema de gestión Bomberos de Bucaramanga operaciones, es un servicio, caracterizado por la

	Sistema de Gestión Bomberos de Bucaramanga Operaciones	atención personalizada, atiende y apoya en forma permanente los requerimientos de la comunidad con criterios de eficiencia y eficacia, basados en la continua modernización tecnológica y organizacional y en el desarrollo integral de nuestros servidores.
4	**Sistema de Gestión Bomberos de Bucaramanga Prevención y seguridad**	El Sistema de gestión Bomberos de Bucaramanga prevención y seguridad, es un servicio, caracterizado por la atención personalizada, atiende y apoya en forma permanente los requerimientos de la comunidad como son visitas a establecimientos comerciales, proyectos de construcción nuevos y antiguos que cumplan con la normatividad vigente, basados en la continua modernización tecnológica y organizacional y en el desarrollo integral de nuestros servidores.

Tabla 4 Módulos del Sistema de Información

8.11 Servicios y productos tecnológicos ofrecidos en la actualidad por Bomberos de Bucaramanga.

El área de TI al interior de la entidad ofrece a sus Stakeholders principales (partes interesadas (usuarios internos y externos), los siguientes productos y servicios TI.

8.11.1 En los puestos de trabajo

- Equipos de cómputo de escritorio
- Licenciamiento para ofimática de la suite de Microsoft Office
- Acceso a internet
- Correo electrónico institucional personalizado
- Sistema telefónico de comunicaciones con extensiones numeradas
- Conexión eléctrica regulada con respaldo total de energía.

8.11.2 En áreas comunes

- Acceso internet a través de red Wi-FI
- Sistema de proyección en la sala de Juntas, sala de crisis y guardia central equipos con puertos VGA y HDMI
- Sistema de control de accesos y asistencia de personal biométrico
- Sistema de vigilancia por circuito cerrado de cámaras

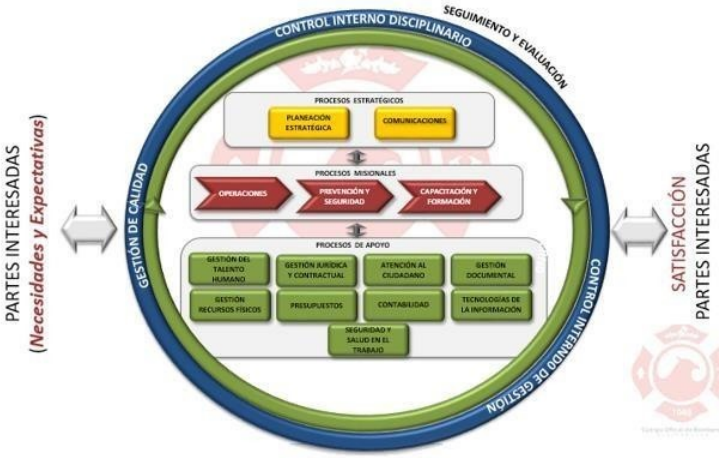
8.11.2 Hacia el ciudadano

Sitio de la página web Bomberos de Bucaramanga, www.bomberosdebucaramanga.gov.co; el cual permite la consulta de información y prestación de servicios de la entidad de interés para el ciudadano como son:

- Pago de servicios mediante el botón de pago,
- Atención al ciudadano link PRQSD, entre otros.
- Línea de atención 119.
- Sistema de vigilancia CCTV para seguridad de los visitantes y usuarios del sistema.

8.11.3 Para los procesos

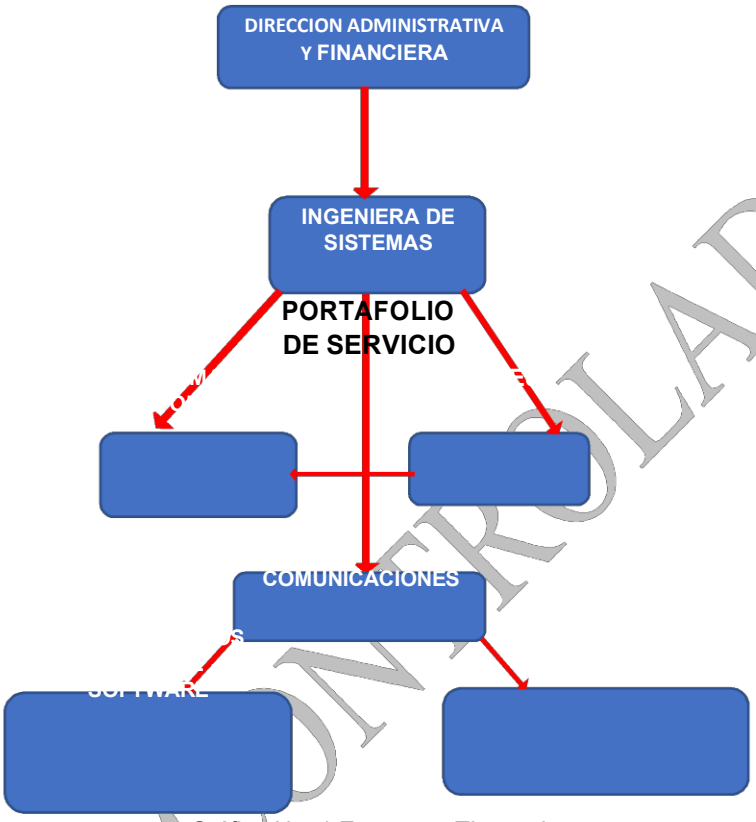
Actualmente la entidad en el proceso que debe adelantar de armonización de los sistemas Calidad y MECI con MIPG, a través del Plan Estratégico de Tecnologías de Información pretende articular la Gestión de Sistemas Informáticos y TIC como un proceso de apoyo (Ver: mapa de procesos articulado con MIPG) Este proceso está a cargo de su implementación y seguimiento por parte de la Dirección Administrativa y Financiera de la entidad, debido a que como podemos observar tanto en la estructura organizacional, como en el mapa de Procesos no está establecido como un proceso y depende de esta Dirección.



Grafica 3 Mapa de Procesos actual

8.11.4 Estructura Actual TI

En la estructura organizacional no se encuentra establecida el área de Tecnologías de la Información, actualmente es coordinada desde la Dirección administrativa y Financiera para la prestación del servicio está apoyada por una Ingeniera de Sistemas-contratista CPS; quien realiza actividades de coordinación del área, presta apoyo en soporte técnico, mantenimientos preventivo y correctivo a los equipos de cómputo, actualizaciones de programas, apoyo a los diferentes softwares de la entidad.



Gráfica No. 4 Estructura TI actual

8.12 Estrategia TI

8.12.1 Objetivo

Evolucionar en el desarrollo de las TI en la entidad, aplicando en la formulación de este dominio los ámbitos de Entendimiento y Direccionamiento estratégico para la implementación, seguimiento y evaluación de la estrategia, desde el entendimiento de la misión, las metas y los objetivos institucionales con el fin de generar valor en la prestación del servicio esencial.

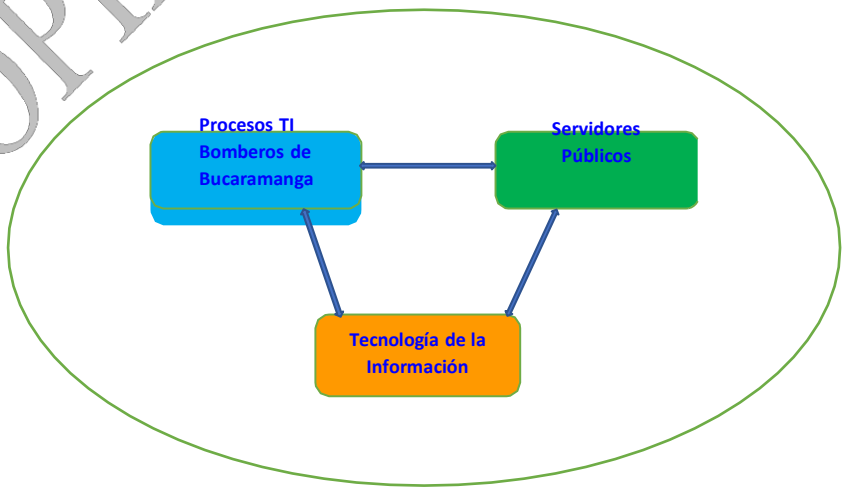
8.12.2 Alcance

Aplica a todos los procesos y funcionarios de la entidad en el uso de tecnología en la ejecución de las actividades misionales y administrativas, que busca facilitar el cumplimiento de entrega de valor en la prestación del servicio esencial.

En la actualidad para que una organización pueda llegar a ser competitiva y eficiente, necesariamente debe estar inmersa las Tics (Tecnologías de Información y Comunicaciones) como parte integral de la planificación estratégica; para alcanzar la visión empresarial de forma rápida y efectiva. Cada vez aparecen nuevas tecnologías, metodologías y mejores prácticas en TI, las cuales se han convertido en la herramienta imprescindible de aplicación para cualquier organización que pretenda desarrollar, mejorar y ser competitiva y que tienen como objetivo fundamental mejorar, en este caso, para Bomberos de Bucaramanga, la prestación del servicio esencial; aplicando con calidad el uso de las TIC, durante y en la prestación del servicio; asociado éste con la creación de valor para incrementar la efectividad en el cumplimiento de la Misión de la entidad. Sin embargo, es necesario precisar que una estrategia de TI pueda lograr los resultados esperados, en cuanto a mejorar la competitividad y desarrollo de la entidad, se requiere proponer, desde una planeación estratégica.

Siendo así, para incursionar la entidad en las tecnologías de la información y velar por el cumplimiento de los planes de Gobierno Digital y aplicarlos a los procesos, es preciso, identificar las necesidades de TI, y plantear un desarrollo de proyectos mediante acciones que contribuyan al logro de estos, teniendo en cuenta que en algunos casos requieren asignación de recursos, o en otros, revisar la oportunidad de aplicar las mejores prácticas; en todo caso, para garantizar el éxito en estos procesos se requiere alinear tres elementos esenciales dentro de la entidad como son los procesos, los servidores públicos y la tecnología, que conllevará a ejecutar la planeación estratégica de forma éxito

8.12.3 Elementos fundamentales para el éxito de la Estrategia



Gráfica No. 5 Elementos fundamentales para el éxito de una estrategia

La estrategia de TI, fue diseñada teniendo en cuenta básicamente, dos variables fundamentales en tecnologías de Información, 1. Tecnología existente en la actualidad y 2. Necesidades que presenta la entidad en este sentido; teniendo un conocimiento del estado actual podremos diseñar las acciones a llevar a cabo para buscar aquellos sectores donde se presentan oportunidades para surtir la dificultad que pueda surgir por la falta de ella, buscando nuevas tecnologías que puedan aumentar la competitividad de la Entidad.

La elaboración de la estrategia involucra tener claro la contribución que cada funcionario realiza desde su puesto de trabajo para el cumplimiento de la misión y de los objetivos institucionales, y como responsable de la ejecución de estas acciones; con este concepto se formularon los objetivos estratégicos compuestos por estrategias, metas y acciones de cómo alcanzarlos en el tiempo y; así, como también tener claro, que es fundamental la asignación de recursos.

8.12.4 Variables para la formulación de la Estrategia TI

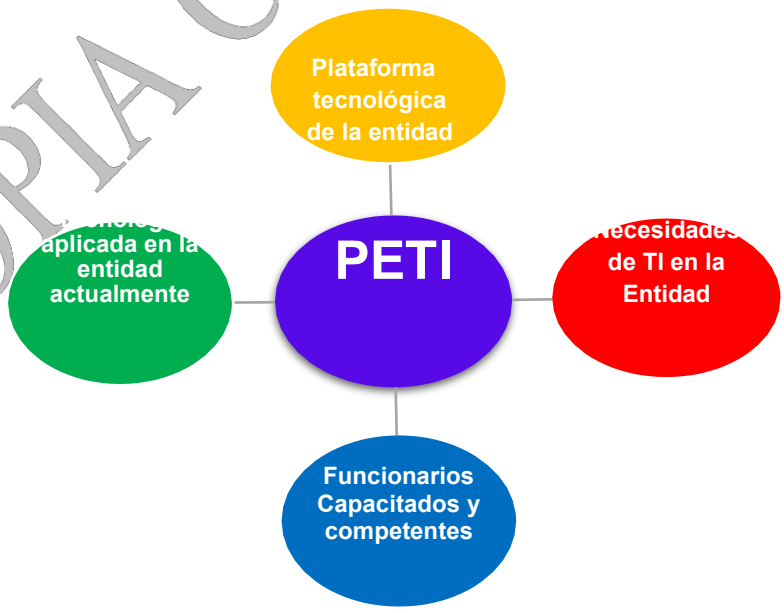


Gráfico No.6 Variables para la formulación de Estrategia TI- Bomberos de Bucaramanga

8.12.5 Necesidades TI

NECESIDADES DE TECNOLOGIAS DE INFORMACIÓN – BOMBEROS DE BUCARAMANGA
1. Sistemas de Información Propios: 1.1 Software Misional 1.2 Software de gestión administrativa. 1.3 Sistema PQRSD y Ventanilla Única
2. Documentar los procesos y procedimientos de TI.
3. Ampliar la plataforma tecnológica: Software y Hardware
4. Confidencialidad y tratamiento de datos.
5. Formación y capacitación en Seguridad de la Información y manejo de programas.
6. Sistema de respaldo de la información
7. Comunicaciones
8. Mantenimiento Preventivo y correctivo de equipos de cómputo, impresoras, escáner, etc
9. Fortalecimiento
10. Licencias de Antivirus
11. Licenciamiento con Microsoft para servicio de correo electrónico institucional

Tabla No.5 Necesidades de Tecnologías

8.12.6 Estrategia TI

Necesidades de TI	Estado Actual	Meta por alcanzar (Requerimientos)	Responsable	CRONOGRAMA														
				Corto Plazo 1 Año												Mediano Plazo		Largo Plazo
				En Meses												2023		2 a 5 años
				Ene	Feb.	Mar.	Abr.	May.	Jun.	Jul	Agos	sept.	Oct.	Nov	Dic.	I SEM	II SEM	
1. Software Misional	No es Propio	Proyecto para adquirir el sistema de información propio, con el objetivo de robustecer la plataforma tecnologica en el segundo semestre de 2022	Dirección General y Dirección Adtiva y Financiera															
1.1 Software administrativo de la entidad (Nomina)	No es Propio	Proyecto para adquirir el sistema de información propio, con el objetivo de robustecer la plataforma tecnologica en el segundo semestre de 2022	Dirección General y Dirección Adtiva y Financiera															
1.2 Sistema PQRSD y Ventanilla Única	Sistema Parcialmente Operativo	1. Aplicar Mejores Practicas 2. Capacitación al usuario por el personal responsable de PQRSD 3. Adquisición Programa PQRSD	Dirección Adtiva y Financiera															
2. Documentar los procesos y procedimientos de TI	No existen	Documentar los procesos y procedimientos dentro del sistema de gestión de calidad enmarcados en el proyecto de modernización de la entidad	Dirección Adtiva y Financiera, responsable Calidad y TI															
3. Ampliar la plataforma tecnologica Software y Hardware	Propuesta para adquisición	Revisión y gestión para adquirir los programas e equipos	Dirección General y Dirección Adtiva y Financiera															
4. Confidencialidad y tratamiento de datos	No existe	Elaborar, aprobar e implementar el plan de mantenimiento de servicios tecnologicos	Dirección General y Dirección Adtiva y Financiera															
5. Formación y capacitación en seguridad de la información y manejo de programas	Correo electronico Institucional	Incluir en el plan Institucional de capacitación para la vigencia 2022, Correos electronicos Institucionales	Dirección Adtiva y Financiera - responsable de Talento Humano															
6. Comunicaciones (Radios, Repetidoras, Avantel, Linea celular, etc)	Es Incipiente	Incluir en el plan Institucional de Compras para la vigencia 2022, como necesidad del area de operaciones	Dirección Adtiva y Financiera - responsable Área de Operaciones															
7. Mantenimiento preventivo y correctivo de equipos de cómputo, Impresoras, escaner, etc	Mantenimiento Anual	Formular e implementar un programa de mantenimiento preventivo de equipos de cómputo, impresoras	Dirección Adtiva y Financiera - responsable TI															
8. Fortalecimiento del área de telemática para cumplir con las condiciones óptimas del área	No existe	Incluir dentro de la ampliación de la plataforma tecnologica compra aire acondicionado de respaldo y que cumpla con las especificaciones técnicas requeridas	Dirección Adtiva y Financiera - responsable TI															
9. Licencias de Antivirus	Se realiza contratación por proceso de Minima cuantía Anual	Incluir en el Plan de compras 2022, como necesidad del área de TI	Dirección Adtiva y Financiera - responsable TI															
10. Licenciamiento con microsoft para servicio de correo electronico institucional	Alojamiento hosting con servicio de correo electronico	Incluir en el Plan de compras 2022, como necesidad del área de TI con el fin de contrarestar la deficiencia en las comunicaciones y perdida de información	Dirección General, Dirección Adtiva y Financiera - responsable TI															

Tabla No.6 Estrategia TI

La estrategia de TI, fue diseñada teniendo en cuenta básicamente, dos variables fundamentales en tecnologías de Información, una la tecnología existente en la actualidad y dos las necesidades que presenta la entidad en este sentido; teniendo un conocimiento del estado actual podremos diseñar las acciones a llevar a cabo para buscar aquellos sectores donde se presentan oportunidades para surtir la dificultad que pueda surgir por la falta de ella, buscando nuevas tecnologías que puedan aumentar la competitividad de la Entidad.

La elaboración de la estrategia involucra tener claro la contribución que cada funcionario realiza desde su puesto de trabajo para el cumplimiento de la misión y de los objetivos institucionales, y como responsable de la ejecución de estas acciones; con este concepto se formularon los objetivos estratégicos compuestos por estrategias, metas y acciones de cómo alcanzarlos en el tiempo y; así, como también tener claro, que debe realizarse la asignación de recursos, de ser necesario.

8.12.7 Estado de las Tecnologías implementadas en Bomberos de Bucaramanga

Para conocer el estado actual en aplicación y uso de TI en la entidad, y después de aplicar una encuesta personalizada al usuario interno en las áreas de Operaciones motor de la entidad y administrativa; las respuestas entregadas sugieren el siguiente estado:

- ✓ La percepción que tienen los funcionarios acerca de TI, se fundamenta en que esta área es la encargada de la sistematización de la información, mantener una página web actualizada, prestar apoyo para dar soluciones a inconvenientes con equipos de tecnología y comunicaciones, apoyo en mantenimientos de hardware, software, búsqueda de información digitalizada de la entidad.
- ✓ El área de TI para toda la entidad está a cargo de una sola persona.
- ✓ El concepto generalizado por los funcionarios entrevistados es que una sola persona en el área de TI, no alcanza a cubrir todas las necesidades requeridas por los procesos de la entidad.
- ✓ Los funcionarios consideran que los servicios que el área de TI presta a la entidad son aquellos que tienen que ver con el acceso y uso de Internet y el correo electrónico, mantenimiento de los PC, impresora y elementos de comunicación, mantenimiento de los sistemas de información, responsabilidad en la actualización de la página web, búsqueda de información histórica de la entidad.
- ✓ En cuanto a los beneficios que el área de TI representa para la empresa no es claro para los funcionarios y se refieren a este, como el apoyo para el funcionamiento físico de los hardware de PC, y de equipos electrónicos; se centran en el beneficio para el funcionamiento en la parte operativa.

- ✓ El área de TI, no cuenta con indicadores claros que sean conocidos por la planta de personal
- ✓ La concepción de la aplicación en un nivel Gerencial estratégico de TI en la entidad es que su uso es limitado, por no contar con una estructura más amplia y una plataforma robusta.
- ✓ Los programas de capacitación no existen para los funcionarios en general, como tampoco para el responsable del área de TI, sin embargo, los usuarios internos de TI, consideran que es necesaria y obligatoria por parte de la entidad dada la naturaleza del manejo permanente de procesamiento y alimentación de Sistemas de información, como el sistema contable y financiero, Sistema de Gestión para las áreas Misionales; así también documentación digital, tanto en formatos de procesamiento de texto como en hojas de cálculo.
- ✓ Existe una percepción en los funcionarios administrativos, operativos y contratistas que la información de gestión administrativa requiere un alto grado de digitación sin embargo esta no es articulada e integrada con los sistemas de información existentes en la entidad.
- ✓ En general todas las áreas de la entidad interactúan para compartir, consultar e intercambiar información, generalmente en procesos informales, correo electrónico y comunicaciones, que conlleva a la duplicidad de información, desgaste administrativo y finalmente la responsabilidad de la información no se establezca con criterio.
- ✓ El concepto de transparencia en cuanto de dar cumplimiento a la Ley 1712 de marzo de 2014. (*El objeto de la presente leyes regular el derecho de acceso a [1 la información pública, los procedimientos para el ejercicio y garantía del derecho y ~ las excepciones a la publicidad de información*), es responsabilidad del área de TI y no de los responsables de los procesos de la entidad para entregar los informes de gestión, así como actualizar el portafolio de servicios y productos de cada proceso. Consideran que la única que debe realizarse es la publicación que se hace de los contratos y documentos exigidos por la reglamentación en las plataformas públicas. [1]
- ✓ En cuanto a mantener una información de cifras y datos estadísticos de la gestión realizada por los procesos de la entidad, especialmente en los procesos misionales en la prestación del servicio misional de Bomberos de Bucaramanga articulados con las partes interesadas como son la comunidad, empresas comerciales, entidades educativas, comunidad en general de áreas urbana y rural requiere un trabajo más integrado y participativo bajo un sistema de información que procure el desarrollo tecnológico y misional integrado.
- ✓ El concepto de los funcionarios del Área de Gestión Documental es que es la gestión es estrictamente operativa, no obedece a ningún criterio estratégico, o de herramientas tecnológicas o programas que tengan como prioridad el apoyo en TI,

[1] Ley Transparencia 1712 de 2014

que puedan dinamizar y automatizar el proceso que contribuyan a desarrollar esta área de manera significativa.

- ✓ La estrategia más implementada en la entidad para interactuar en los procesos en cuanto a entradas y salidas de información, como insumo para otros procesos es mediante el correo electrónico, considerándolo una forma de protección de datos.
- ✓ La estructura para protección de datos y copias de seguridad no están establecidos mediante procedimientos documentados, por tanto, no son claros para la mayoría de los funcionarios entrevistadas, por tanto, en su gran mayoría las acciones tomadas para preservar y proteger la información generada son mediante la elaboración de actos administrativos y el correo electrónico, los cuales consideran minimizan los riesgos personales en ejercicio de sus funciones.

8.13 SISTEMAS DE INFORMACIÓN

Inventario de los sistemas de información de los que dispone la entidad en el Área Administrativa y en el Área de Operaciones para la prestación del Servicio misional en la prevención y atención de emergencias en Bomberos de Bucaramanga.

No.	Nombre de sistema de información	Sigla	Descripción	Derechos patrimoniales
1	Global Businnes Solution	GBS	Sistema contable	GBS
2	Página Web			Bomberos
3	Correo		Correo electrónico	Camino Web
4	Directorio Activo		Activación de Usuario	Contrato
5	Sistema de Gestión Bomberos		Sistema de gestión de emergencias, programación de visitas a inspecciones, y capacitaciones	GEA Soluciones
6	Software de Gestión CrossChex Standard –		Sistema de control entrada y salida de personal por huella	Software Libre
7	Pasivocol		Software de Ministerio de Hacienda y crédito Público (Historias laborales de activos y retirados).	
8	Radios Digitales – Bomberos	TRBOnet	software para monitoreo de radios	Software libre – Bomberos.

Tabla 7 Sistemas de Información disponibles en Bomberos de Bucaramanga

8.13.1 Estructura organizacional requerida para el área TI

Se requerirá de una estructura que permita la planeación de las necesidades de los usuarios internos y de los usuarios externos:

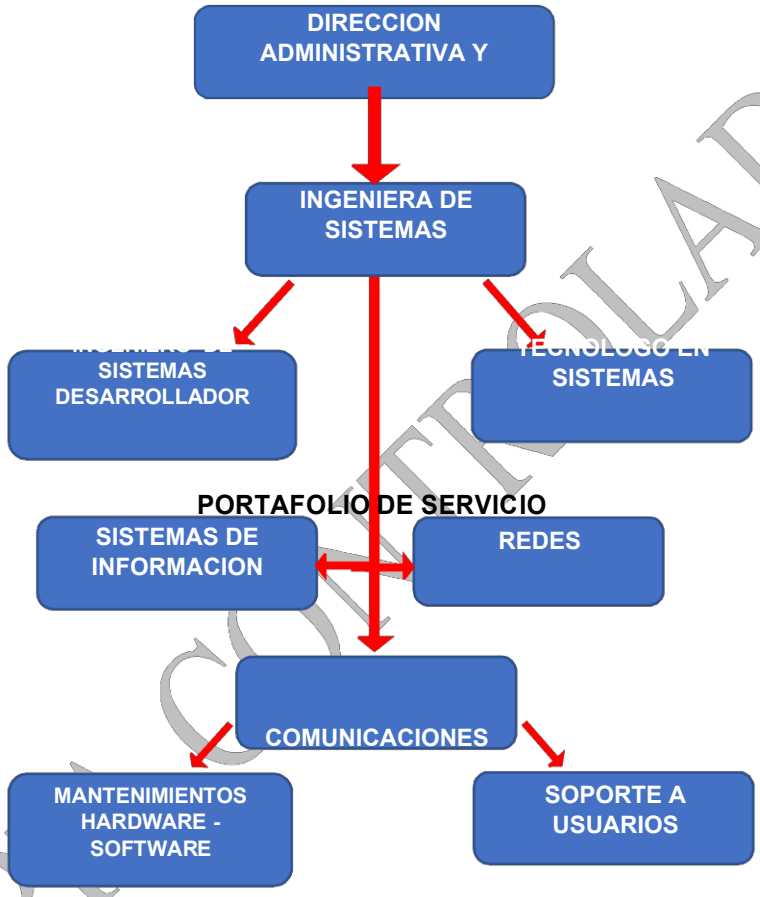


Ilustración 1 Estructura Organizacional requerida para TI

En la actualidad no existe personal de planta que coordine el área de sistemas, la responsabilidad de todo el proceso recae sobre una sola persona de contrato de prestación de Servicios, que depende de la Dirección Administrativa Financiera.

Para la ejecución del presente PETI se requiere entonces durante los siguientes 40 meses, migrar a una estructura de 3 personas, teniendo como base administrativa el esquema funcional de un responsable del área TI, que continuará dentro de la Dirección Administrativa y Financiera, en actividades principales de coordinación, y mejoramiento en la aplicación de herramientas tecnológicas y automatización de los procesos esenciales como por un ejemplo de los muchos existentes, Gestión Documental que requieren ser modernizados, mediante la aplicación de las mejores prácticas en procesos tan operativos; así como también el seguimiento del trabajo de dos personas más (por ejemplo convenio con universidades para pasantes o practicantes), con el

acompañamiento de un especialista Desarrollador para apoyar actividades en el desarrollo de nuevas tecnologías y programación de nuevas aplicaciones o programas para el fortalecimiento institucional. Así mismo, se requiere para actividades con perfiles de tecnólogo o técnico para actividades operativas en el apoyo en Infraestructura y Soporte técnico para el área administrativa y procesos misionales.

Este esquema permitirá que vaya adquiriendo un mayor control en el gobierno digital y gestión de los recursos TI. Así mismo, esta estructura irá preparando a la entidad para procesos de innovación y cambio. Esta es una necesidad que es preciso identificar; en cuanto a la formalización de un equipo especializado en TI, que contribuya en el desarrollo y fortalecimiento de esta área en la entidad.

Esta es una estructura mínima necesaria para la puesta en marcha del PETI y cumplimiento de las obligaciones TI a cargo de la entidad, y ha sido considerada dentro de las capacidades presupuestales, ya que dependen en gran medida de la gestión Gerencial que pueda realizarse y contribuyen de manera significativa para el desarrollo y dinamismo en los procesos de la entidad para la atención de los requerimientos de apoyo y soporte técnico en las áreas.

8.14 ESTRATEGIAS Y PRINCIPIOS PETI BOMBEROS DE BUCARAMANGA

8.14.1 Tipo de Estrategia Requerida

La entidad requiere en gran medida, en aras de un avance significativo la aplicación y uso de herramientas tecnológicas que contribuyan al desarrollo y modernización en los procesos y en la gestión realizada para dar cumplimiento a los planes de gobierno digital tanto a nivel normativo, como en la aplicación de las mejores prácticas que le aporten creación de valor en la prestación del servicio y en los procesos administrativos.

Es por ello, que es preciso formular una estrategia dinámica y eficiente en cuanto a las necesidades TI. Hasta el momento la gestión realizada en este proceso ha sido de tipo reactiva. Para la ejecución de esta estrategia requerirá de una estructura que permita la planeación, ejecución, la evaluación de la efectividad de las acciones implementadas y de los recursos asignados, y en el caso que sea necesario plantear un plan de acción que mejore el proceso de TI y satisfaga las necesidades y requerimientos de los usuarios internos y de los usuarios externos en los niveles de:

1. Sistemas Software y Sistemas de Información
2. Hardware
3. Redes internas y de comunicaciones
4. Confidencialidad y tratamiento de los datos
5. Implementación de la Política de Seguridad de la Información
6. Formación y capacitación del recurso humano para optimizar los beneficios del sistema.

8.14.2 Procesos requeridos

La ejecución de la estrategia PETI para los siguientes dos años exigirá la creación y documentación de los siguientes procesos clave:

- Procedimientos de Gestión TI
- Manuales de Funciones Roles TI
- Manual de Desarrollo de nuevas aplicaciones.
- Servicios de soporte técnico y funcional
- Plan de Contingencia para TI
- Procedimientos soporte técnico y mesa de ayuda
- Procedimientos de asignación y uso de activos digitales
- Procedimiento para manejo de datos

8.14.3 Roles a desempeñar para la ejecución del PETI

Dentro de las funciones del esquema del plan estratégico TIC el siguiente es el resumen de las funciones según el rol:

ROLES	ACTIVIDADES PETI
Responsable TI	Planes estratégicos de Gestión TI
	Desarrollo de actividades en la Gestión de Gobierno Digital
	Coordinación, desarrollo de nuevas tecnologías, programación y mejoramiento en la aplicación de herramientas tecnológicas, automatización y desarrollos tecnológicos
Gestión Proyectos TI	Portafolio de Planes y Proyectos 2020-2023
	Capacitación planificada desde PIC dirigida a funcionarios responsables del área TI, usuarios internos.
	Seguimiento a Gestión de Proveedores
	Plan de Contingencia para TI
	Procedimiento para soporte técnico y mesa de ayuda
	Procedimiento para operación de tareas repetitivas
	Procedimientos para copias de seguridad
Seguridad de Información	Componente Gobierno Digital
	Transparencia de la información Ley 1712 de 2014
	Políticas de Privacidad y Seguridad de la información
	Mecanismos de uso, aplicación y acceso a la información
	Arquitectura de Sistemas de Información

ROLES	ACTIVIDADES PETI
	Interconexión
	Interacción de Comunicaciones
Sistemas de Información	Acuerdos de Servicio y de desarrollo
	Plataformas electrónicas de comunicaciones con la comunidad
	Arquitectura de Infraestructura tecnológica
Servicios Tecnológicos	Portafolio de Servicios
	Acceso WI-FI al ciudadano en el SITM y las oficinas administrativas
	Desarrollo de proyectos TI 2020 y 2023 como Proyectos de inversión en Plan de compras aprobado.
	Servicios de soporte técnico y funcional para usuarios internos administrativos y Áreas Misionales.
	Interconexión
	Planes de Contingencia TI para la entidad
	Servicios de administración y operación
	Procedimientos soporte técnico y mesa de ayuda
Seguimiento y control Estrategia TI	Medición de niveles de adopción de TI y satisfacción
	Políticas, Estándares y lineamientos TI
I+D+I (Investigación + Desarrollo + Innovación)	Uso y aplicación generalizado de la tecnología de la información en todos los procesos, funcionarios de la entidad, partes interesadas articulados con los sistemas de información.
	Promover la innovación y creación de valor en los procesos mediante la aplicación de nuevas tecnologías.
	Prestación de servicios / productos/ servicios Innovadores

Tabla 8 Roles para la ejecución del PETI

8.14.4 Tecnologías de apoyo requeridas

Niveles de soporte y servicios

Para el cumplimiento de la Misión Institucional es necesario tener establecidos e interiorizados cuales son los niveles de servicio en el estricto concepto de prevención, seguridad y atención integral del riesgo; por ello, la necesidad de contar con una claridad de los niveles del servicio es fundamental tanto del personal que presta el servicio, como del administrativo que presta apoyo en el sentido de la demanda/requerimientos de la comunidad frente a la efectividad en la entrega del servicio de Bomberos de Bucaramanga.

8.14.5 Servicios TI ofertados al interior de Bomberos de Bucaramanga en servicios actuales.

Es, por tanto, responsable de brindar orientación al usuario sobre el uso de los recursos Software, Hardware y Comunicaciones que existan en la entidad para prestación del servicio misional. Así como, es prioridad del equipo de soporte de TI garantizar que los sistemas de información y todos sus elementos, operen en la medida requerida por la entidad e igualmente dentro de las condiciones y políticas de seguridad establecidas, de acuerdo con sus políticas. (Ver: Políticas de seguridad y privacidad de la información).

La intervención en soporte TI para los procesos misionales y administrativos es pertinente dada la necesidad en la prestación del servicio de atención y prevención de incendios, un quehacer que de por medio está salvaguardar y preservar la vida, por lo cual, la necesidad de disponer de una unidad o un equipo humano que dominen y apliquen hasta el mínimo recurso TI en la entidad como sinónimo de eficiencia en el manejo de los recursos en función de los usuarios. Así mismo es responsable de brindar orientación al usuario sobre el uso de los recursos Software, Hardware y Comunicaciones que existan en la entidad. Así mismo es función del equipo de soporte garantizar que estos componentes de los sistemas de información operen en la disponibilidad requerida por la entidad e igualmente dentro de las condiciones y políticas de seguridad establecidas (Ver: políticas de seguridad y privacidad de la información).

8.14.6 Canales de prestación del servicio TI y personal disponible

Para la prestación del servicio en el área TI, solo existe una persona encargada del proceso de Tecnología, y se tiene acceso para los servicios de soporte, mediante comunicaciones vía correo electrónico, telefónica, WhatsApp o de la forma más tradicional mediante una visita a la oficina de sistemas que es la encargada.

A partir de la formulación e implementación del PETI, los canales de prestación del servicio TI deben fluir de manera más perceptible por los usuarios tanto internos como externos, la información requiere ser confiable, oportuna, transparente y disponible en la plataforma tecnológica.

8.14.7 A nivel comunidad

- Es necesario encontrar mecanismos que coadyuven en facilitar el acceso a la información, en primer lugar, para dar cumplimiento a la Ley 1712 de 2014, “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la

Información Pública", porque es un derecho que tiene el ciudadano como método de rendición de cuentas, de hacer transparente la gestión pública.

- La optimización de los sistemas de información que son accedidos directamente por los ciudadanos en función de la comodidad, usabilidad, facilidad de acceso a los mismos, así como dar aplicabilidad a la ley anti trámites, que garantizan la accesibilidad a la información como un recurso que el ciudadano espera obtener de forma gratuita y oportuna.

8.14.8 La tecnología y las comunicaciones

Es necesario mejorar las comunicaciones con los usuarios internos y externos a través de la tecnología. Debe ser pretencioso el objetivo en buscar que la tecnología contribuya al mejoramiento de la gestión, apoyando los procesos para alcanzar una mayor eficiencia y transparencia en el proceso de ejecución de las actividades que desarrollan los procesos en la entidad, de tal manera que facilite la administración y el control de los recursos y que brinde información objetiva y oportuna para la toma de decisiones en todos los niveles. Cuando las comunicaciones fluyen de manera asertiva permite la alineación de la gestión de TI con los objetivos estratégicos de la entidad, a su vez permite aumentar la eficiencia y mejorar la forma como se presta el servicio esencial

Cuando la tecnología y las comunicaciones se articulan de manera adecuada mediante el uso innovador y creativo de la información que se publica al ciudadano, y permite desarrollar una gestión de TI que genere valor estratégico para Bomberos de Bucaramanga y la comunidad, que espera recibir un servicio impecable cuando desafortunadamente acude al llamado de emergencia, este debe ser acorde con las expectativas que genera la preservación de la vida; teniendo como fortaleza la experiencia y el conocimiento de la entidad y las personas que la conforman.

Finalmente, en términos de efectividad e innovación, es importante tener una forma de hacer las cosas bajo los principios de planeación en la acción, es decir, que existen tiempos para planear, tiempos para ejecutar y tiempos para mejorar.

8.15 PROTOCOLO DEL PROCEDIMIENTO DE MANEJO DE LAS TIC

Para la mejora, desarrollo y fortalecimiento del proceso TI en Bomberos de Bucaramanga se describirán los procedimientos requeridos que incluyen el entendimiento estratégico de la Arquitectura Empresarial.

Los procedimientos que se deben documentar en el proceso de TI, se enumeran a continuación, éstos constituyen una base sólida para que la entidad genere sus documentaciones teniendo en cuenta las características particulares, sus activos de información, sus procesos y los servicios de información que presta durante la prestación del servicio misional. Con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad, se toman en cuenta algunos numerales que

pueden impactar en el control de seguridad de la información definidas en la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios.

Es preciso, enfatizar que estos deben ser elaborados por el responsable o coordinador del proceso quien es el que conoce el que hacer y las actividades que se deben incluir, así como articular las políticas de las Tecnologías de Información con esta documentación de tal manera que ayuden a la correcta gestión de los activos de información de la entidad.

Es ideal incluirlos y parametrizarlos en el Sistema de Gestión de la Calidad de la entidad para que sean interiorizados, socializados e implementados de manera estandarizada a través de un sistema para toda la entidad con el acompañamiento y monitoreo continuo del área de sistemas. Por lo anterior, se deben documentar los siguientes procedimientos:

AREA	NOMBRE PROCEDIMIENTO	C0NCEPTUALIZACIÓN
SEGURIDAD DEL RECURSO HUMANO Relacionado con el personal que labora dentro de la entidad, se pueden definir los siguientes procedimientos	**1.PROCEDIMIENTO DE CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL.**	Indica la metodología empleada por la entidad para realizar la capacitación y sensibilización del personal en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades, la periodicidad de dichas capacitaciones y sensibilizaciones etc
	2.PROCEDIMIENTO DE INGRESO Y DESVINCULACIÓN DEL PERSONAL	Indica la manera como la entidad gestiona de manera segura el ingreso y desvinculación, incluyendo temas como verificación de antecedentes, firma de acuerdos de confidencialidad. Para este procedimiento puede generarse colaboración con el área de contratación y de Recursos humanos o contratación.
GESTION DE ACTIVOS Relacionado con la identificación y clasificación de activos de acuerdo a su criticidad y nivel de confidencialidad, se pueden definir los siguientes procedimientos	**1.PROCEDIMIENTO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS**	En este procedimiento se debe indicar la manera en que los activos de información son identificados e inventariados por la entidad, así como también se debe especificar como son clasificados de acuerdo a su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral con la entidad. Así mismo, se debe explicar cómo se hace una correcta disposición de los activos cuando ya no se requieran y su transferencia hacia otros puntos estratégicos de manera segura.
CONTROL DE ACCESO	**1.PROCEDIMIENTO PARA INGRESO SEGURO A LOS SISTEMAS DE INFORMACIÓN**	En este procedimiento la entidad debe indicar como gestiona el acceso a sus sistemas de información de manera segura, empleando métodos preventivos contra ataques de fuerza

AREA	NOMBRE PROCEDIMIENTO	C0NCEPTUALIZACIÓN
Relacionado con el acceso a la información y a las instalaciones de procesamiento de la información, se pueden generar los siguientes procedimientos.		bruta, validando los datos completos para ingreso a los sistemas, empleando métodos para cifrar la información de acceso a través de la red entre otros.
	2. PROCEDIMIENTO DE GESTIÓN DE USUARIOS Y CONTRASEÑAS	En este procedimiento, la entidad deberá indicar como realiza la creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas seguras definida previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente, llevando un registro de las mismas. Este procedimiento debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.
SEGURIDAD FÍSICA Y DEL ENTORNO relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información. Se pueden generar los siguientes procedimientos (estos procedimientos pueden tener la participación del área de seguridad y vigilancia de la entidad):	**PROCEDIMIENTO DE PROTECCIÓN DE ACTIVOS**	Este procedimiento debe contener los pasos con los cuales los equipos son protegidos por la entidad. Se recomienda que este procedimiento indique como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran las instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas etc.
	PROCEDIMIENTO DE RETIRO DE ACTIVOS	En este procedimiento debe especificarse como los activos son retirados de la entidad con previa autorización. Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos etc.…).
SEGURIDAD DE LAS OPERACIONES	**PROCEDIMIENTO DE GESTION DE CAPACIDAD**	Se debe especificar como la organización realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son escasos, demorados en su arribo o costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda etc.…

AREA	NOMBRE PROCEDIMIENTO	C0NCEPTUALIZACIÓN
Busca asegurar las operaciones correctas dentro de las instalaciones de procesamiento de información.		
	PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	La entidad debe indicar por medio de este procedimiento como realiza la protección contra códigos maliciosos teniendo en cuenta, que controles utiliza (hardware o software), como se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo.
SEGURIDAD DE LAS COMUNICACIONES	**PROCEDIMIENTO DE TRANSFERENCIA DE INFORMACIÓN**	En este procedimiento la entidad deberá indicar cómo realizar la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción. Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan, condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	**PROCEDIMIENTO ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE**	Este procedimiento deberá describir como se realiza la gestión de la seguridad de la información en los sistemas desarrollados internamente (inhouse) o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad. Dicha gestión y control también debe ser especificada para los sistemas ya existentes que son actualizados o modificados en la entidad. Se deben tener en cuenta el uso de ambientes de desarrollo, pruebas y producción para los sistemas de información.
	PROCEDIMIENTO DE CONTROL SOFTWARE	En este procedimiento la entidad deberá indicar como realiza el control de software, es decir, como limita el uso o instalación de software no autorizado dentro de la entidad, quienes están autorizados para realizar la instalación de

AREA	NOMBRE PROCEDIMIENTO	C0NCEPTUALIZACIÓN
		software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.
GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**PROCEDIMIENTO DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	Este procedimiento debe indicar como responde la entidad en caso de presentarse algún incidente que afecte alguno de los 3 principios fundamentales de la información: Disponibilidad, Integridad o confidencialidad. Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los planes de BCP (Planes De Continuidad) dependiendo de la criticidad de la información.
COPIAS DE SEGURIDAD O BACKUPS	**POLITICAS Y PROCEDIMIENTOS DE RESPALDO DE DATOS**	Este procedimiento está enfocado al respaldo de la información o los datos en caso de presentarse un incidente como virus informático, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, inundaciones, incendios en donde se realizará un análisis previo del sistema de información o datos a respaldar, en el que se definirán las medidas técnicas, el tiempo disponible para efectuar la copia, los dispositivos magnéticos, ópticos, extraíbles a utilizar para realizar la copia, se debe tener en cuenta la frecuencia de realización de la copia de seguridad y las medidas de seguridad respecto a las copias de seguridad que es la de verificar la correcta aplicación de los procedimientos de realización de las copias de respaldo y recuperación de los datos.

Tabla 9 procedimientos documentados para TI

Para el proceso de Tecnologías de Información es necesario estandarizar algunas actividades que hacen parte de procesos sensibles para la seguridad de la información y que aseguren que el proceso se realice de manera adecuada; garanticen y den confianza que se realiza de la manera como fue planificada.
Así mismo se requiere documentar el Plan de Contingencia TI.

8.15.1 Política para la gestión eficiente de la información

Las políticas de Seguridad y Privacidad de la Información fueron adaptadas para Bomberos de Bucaramanga durante la elaboración del PETI por ser una política

fundamental y de cumplimiento; por lo cual la entidad deberá implementarla de manera inmediata para su uso seguro y eficiente de los activos de información.

8.15.2 Políticas de seguridad y privacidad de la información

La información es un activo valioso que facilita la toma de decisiones, la continuidad de la operación, la mejora en los procesos de la entidad, facilita la rendición de cuentas y respuestas a la comunidad, a entes de control, así como compartir y darle trascendencia al conocimiento.

Por lo anterior, la necesidad de mitigación de riesgos alrededor de la información es imperativa, por eso se requieren planes de manejo de incidentes y herramientas para proteger dicha información.

Al formular el Plan estratégico de tecnologías de la información (PETI) para la vigencia 2020 – 2023, se elaboró la Política de Seguridad y privacidad de la información para Bomberos de Bucaramanga, con el propósito de proteger y preservar la información de la entidad, la cual se relaciona a continuación y que está sujeta a su aprobación, adopción e implementación:

8.15.3 Objetivo general

Preservar, mantener y disponer la información como el activo más valioso para Bomberos de Bucaramanga, tomando las precauciones para proteger los principios fundamentales de seguridad de la información como son la **Confidencialidad, Integridad y Disponibilidad**; así como adoptar las buenas prácticas, en cuanto a la gestión y administración de las tecnologías de la información, para interiorizarla, implementarla y resguardarla.

8.15.3.1 Objetivos específicos

Bomberos de Bucaramanga, con el objetivo de cumplir su misión, visión y procesos estratégicos, y soportar las actividades o funciones de seguridad de la información como:

1. Cumplir con los principios de la seguridad de la información.
2. Mantener la confianza de los funcionarios, contratistas, practicantes y de sus clientes.
3. Proteger los activos tecnológicos de la entidad y la información.
4. Establecer un procedimiento en materia de seguridad de la información.
5. Fortalecer la cultura de seguridad en los funcionarios, contratistas y practicantes de Bomberos de Bucaramanga, mediante sensibilización, y capacitación.
6. Garantizar la preservación y disponibilidad de la información frente a los incidentes.
7. Cumplir con los principios de seguridad y privacidad de la información: disponibilidad, integridad y confidencialidad.
8. Concientizar a los funcionarios, contratistas, practicantes de Bomberos de Bucaramanga sobre el uso adecuado de los activos de información puestos a su disposición para el desarrollo de sus funciones y actividades del día a día, garantizando los tres pilares de la información confidencialidad, la privacidad y la integridad de la información.

9. Dar cumplimiento a los lineamientos de Gobierno Digital respecto a la Seguridad de la información.
10. Establecer un Plan de contingencia para TI.

8.15.4 Alcance:

La política de Privacidad y Seguridad de la información aplica a toda la entidad, funcionarios, contratistas, practicantes, personal externo que cuente con un equipo conectado a la red de Bomberos de Bucaramanga, que tengan acceso a la información a través de los documentos, equipos de cómputo, infraestructura tecnológica y medios de comunicación de la entidad. La Política de Seguridad y privacidad de la Información de la entidad, coordina y controla la gestión necesaria para mitigar los riesgos.

8.15.5 Nivel de cumplimiento

Todas los funcionarios y procesos cubiertos por el alcance de la política de seguridad y aplicabilidad se espera que se aplique en un 100%.

8.15.6 Políticas de seguridad y privacidad de la información

Bomberos de Bucaramanga determina definir, adoptar, aplicar e implementar una Política de Privacidad y Seguridad de la información, alineada con la Misión, Visión y Objetivos de la entidad.

- Bomberos de Bucaramanga, se compromete a proteger, preservar, y mantener la información que se genera en la ejecución de sus funciones, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las diferentes dependencias, funcionarios, contratistas, practicantes y toda persona que interactué con la información y la utilicé físicamente o a través de equipos, medios de almacenamiento, plataformas, o sistemas de información dispuestos para su gestión.
- Bomberos de Bucaramanga, protege la información creada, procesada y distribuida por los procesos de su competencia, infraestructura tecnológica, activos de información, que se genera con los accesos otorgados a terceros (contratistas, practicantes, proveedores internos y externos o ciudadanía en general).
- Bomberos de Bucaramanga, protege la información creada, procesada, transmitida por sus procesos de operación, con el fin de proteger la información financiera, operativa o legal debido a un uso incorrecto de la misma.
- Bomberos de Bucaramanga debe proteger la información de amenazas que se puedan originar por parte de sus funcionarios, contratistas, practicantes, usuarios o la ciudadanía en general.
- Bomberos de Bucaramanga debe garantizar el cumplimiento de sus obligaciones legales, o contractuales establecidas.

- Los lineamientos frente a la seguridad y privacidad de la información de Bomberos de Bucaramanga son definidas, compartidas, adoptadas, publicadas y deberán ser aceptadas mediante la firma en las actas de asistencia o carta de compromiso en la socialización, interiorización e implementación de la política de seguridad y privacidad de la información promovida por la Dirección Administrativa y Financiera y retroalimentada en el programa de inducción y reinducción dirigida a los funcionarios, contratistas o practicantes de la entidad.

8.15.7 control de los activos de la entidad

- Bomberos de Bucaramanga coloca a disposición de los funcionarios, contratistas y practicantes, el uso de los equipos necesarios para la realización de las labores propias de los respectivos cargos.

- Todos los funcionarios, contratistas u practicantes que usen los activos de información que sean propiedad de Bucaramanga son responsables de cumplir y acogerse con la integridad de esta política de uso aceptable para dar un uso responsable y eficiente a los recursos asignados.

- Bomberos de Bucaramanga es propietario de los activos de información y los administradores de estos activos son los funcionarios. Contratistas, Practicantes (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware, o infraestructura de tecnología y sistemas de información (TIC).

8.15.8 Políticas de uso y acceso a los equipos

8.15.8.1 Acceso de los usuarios

Todo acceso a los equipos y sistemas de información estará controlado y autorizado por el administrador de sistemas y la Dirección General. Es de carácter condicional y restringido para los usuarios, intentar acceder a los sistemas o recursos a los que no tenga autorización expresa de los mismos.

Los usuarios se comprometen a respetar los derechos de terceros en los sistemas de uso compartido, comprometiéndose en el presente documento a no modificar, eliminar la información privada de otros usuarios, sin previa autorización. Asimismo, los usuarios se comprometen a no compartir ficheros o documentos de cualquier tipo con otros usuarios, sin implementar las medidas necesarias que garanticen la seguridad de la información y de los sistemas operativos.

Todo usuario autorizado tiene acceso a los sistemas informáticos mediante un nombre de usuario y contraseña personal e intransferible, comprometiéndose a tratarla con la

máxima diligencia y confidencialidad, siendo el único responsable del buen uso de la misma. El titular autorizado será responsable único y directo de todo lo ejecutado en el sistema bajo su nombre de usuario y contraseña. Asimismo, se deben evitar los intentos reiterados, por cualquier medio, para obtener el acceso a contraseñas de otros usuarios sin su consentimiento.

Los usuarios no están autorizados a divulgar por cualquier medio las claves de acceso a cualquiera de los servicios que se faciliten a los empleados. Todos los nombres de usuario, contraseñas, claves de acceso y demás identificadores facilitados al usuario tendrán el carácter de confidencial, resultando personales e intransferibles. Los usuarios se comprometen a dar aviso al administrador de sistemas y/o al responsable de seguridad de forma inmediata de cualquier incidencia o anomalía detectada en los accesos a los sistemas de información o en la seguridad de los mismos.

Se sugiere a los usuarios no instalar software que no sean licenciados en equipos de propiedad de la entidad.

8.15.9 Accesos del administrador de sistemas

El administrador de sistemas se obliga a actuar con absoluta diligencia, guardando total confidencialidad sobre los datos, documentos, y demás informaciones a las que pudiere tener acceso en el ejercicio de sus tareas. A título ejemplificativo, pero no limitativo se pueden incluir los siguientes:

Acceso a los equipos y sistemas de información para llevar a cabo tareas de mantenimiento.

Acceso a los equipos, sistemas de información y documentos electrónicos por motivos de seguridad.

Autorizar los accesos de los usuarios a los sistemas de información que requieren para el cumplimiento de sus tareas, así como a los equipos informáticos, en conjunto con el responsable de seguridad.

Acceso a los equipos, redes o sistemas de información por incidencias en la seguridad de la información.

En cualquier caso, el administrador de sistemas tiene el deber y la obligación de guardar con absoluta confidencialidad toda la información a la que tengan acceso para el cumplimiento de sus actividades, quedando estrictamente prohibido comunicarla o facilitarla, DIRECTA O INDIRECTAMENTE A NINGÚN TERCERO.

8.15.10 Asignación de claves y políticas de contraseñas

8.15.10.1 Procedimientos de asignación de contraseñas y control de acceso.

Cada usuario con acceso autorizado a los medios tecnológicos de la institución, dispondrá de un nombre de usuario personalizado para su identificación, así como de una

contraseña para autenticarse a los sistemas de información, las claves son de uso personal e intransferible.

La comunicación al usuario de su nombre de usuario o login y su contraseña o password será proporcionada por el responsable de seguridad, quien lo comunicará personalmente o mediante correo interno, garantizando en todo caso su confidencialidad y secreto, facilitando al usuario la posibilidad de modificar posteriormente dicho nombre de usuario y contraseña, las cuales son vigentes en la organización hasta el momento de culminación de las relaciones contractuales.

Se prohíbe a todos los funcionarios, contratistas, practicantes de la entidad el préstamo y/o divulgación de las claves asignadas, o el uso de claves de otros usuarios.

Cuando ingresa nuevo personal, la solicitud de cuenta de usuario debe ser solicitada por el jefe del área. Los cambios de privilegios o accesos serán solicitados por el jefe inmediato del empleado.

Los terceros (contratistas, proveedores con privilegios de acceso remoto a la red corporativa) que requieran acceso al software y/o aplicaciones, deben estar debidamente autorizados por la Dirección General.

Privilegios de administración de usuarios como borrar, modificar, solo debe otorgarse al área de TIC de la entidad.

Los usuarios y las contraseñas del personal que se retira de la entidad, deben ser eliminados. Para ello el encargado de las copias de seguridad deberá realizar la debida copia en el medio de almacenamiento dispuesto para tal fin.

La Dirección Administrativa y Financiera es el área encargada de informar oportunamente al área de Telemática la novedad de retiro e ingreso de personal.

Los usuarios no pueden reutilizar contraseñas configuradas anteriormente para el ingreso de los sistemas.

Las claves o contraseñas deben:

Tener mínimo ocho (8) caracteres alfanuméricos.

Las contraseñas no pueden tener el mismo nombre de la cuenta de usuario ni el nombre completo.

La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo: ¡, $, %, &, *)

La caducidad de las contraseñas es de 45 días, y al usuario el sistema le notificará 3 días antes de expirar el cual cada usuario deberá cambiar la contraseña por una nueva.

Al crear la cuenta por primera vez se debe configurar para que el usuario cambie la contraseña en el primer inicio de sesión.

8.15.11 Recursos compartidos

La utilización de carpetas compartidas con los usuarios, son prácticas para mantener la información estructurada por dependencias, este tipo de herramienta es útil para el trabajo diario, por lo tanto, su uso y aplicación debe ser controlado para mantener los principios de confidencialidad, integridad y disponibilidad de la información. Con este propósito se definen los siguientes lineamientos para su uso seguro:

- El usuario que se autoriza y dispone de los recursos compartidos de la entidad, es responsable por las acciones y los accesos sobre la información del contenido de la carpeta.

- Dependiendo del tipo de acceso y rol solicitado se darán los permisos sobre la carpeta compartida (lectura, escritura, modificación y borrado).

- Especificar el límite de tiempo, el cual estarán disponibles en la red los recursos compartidos en el equipo del usuario.

- El responsable de la seguridad de la información de la entidad no se hace responsable **por el uso inapropiado del repositorio ni tampoco se hace custodio de la información allí contenida**, puesto que todos los usuarios de la red van a tener acceso a dicha unidad con privilegios de crear, modificar, borrar, leer todos los elementos allí contenidos.

- El objetivo de este repositorio es mejorar la eficiencia y el impacto ambiental reduciendo el uso de papel e impactar de manera positiva sobre factores económicos y administrativos en la entidad.

- El repositorio o carpeta compartida es de uso temporal, solo para transferencia de información entre usuarios; por lo tanto, cada usuario debe manejar la información en el disco duro del equipo asignado, lo anterior con el fin de evitar perdida de datos.

8.15.12 Política de uso de impresoras, fotocopiadoras, scanner y del servicio de impresión.

Asegurar la operación correcta y segura de las impresoras, fotocopiadoras, scanner y del servicio de impresión.

Los documentos que se impriman en las impresoras de Bomberos de Bucaramanga deben ser de carácter institucional.

Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al encargado del área de telemática de la entidad.

Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada, debe mantener control de la impresora, evitando que personal ajeno tenga acceso a ella, para preservar el principio de la confidencialidad de la información.

8.15.13 Gestión de incidencias

Todas las incidencias en la utilización de los recursos y medios tecnológicos de la institución, o que, por cualquier circunstancia, directa o indirecta pueda comprometer la Seguridad de la Información, deberá ser notificada con la mayor brevedad que sea posible al responsable de seguridad.

El responsable de seguridad será el encargado de llevar a cabo un registro, diagnóstico y seguimiento de todas las incidencias comunicadas por los usuarios. Asimismo, deberá mantener actualizado el registro de incidencias donde se especificará el tipo de incidencia y la resolución de las mismas, comprobando periódicamente que las incidencias son resueltas y la Seguridad de la Información queda garantizada.

8.15.14 Seguridad, confidencialidad y protección de datos personales

Toda la información contenida en los equipos informáticos, correo electrónico, dispositivos de almacenamiento y demás sistemas de información son de carácter privado y confidencial. La obtención de datos de carácter personal sin autorización, así como la violación de la privacidad y confidencialidad de la información por parte del personal, constituyen faltas sancionadas por la normativa vigente.

En el presente documento las partes se comprometen a guardar el secreto de las comunicaciones, respetar la privacidad y confidencialidad de todos los datos e informaciones, y no ceder a terceros los datos e información de carácter personal obtenidos en el cumplimiento de sus actividades directas o cualesquiera otras del ámbito institucional, de conformidad con la ley de Protección de Datos de Carácter Personal LEY 1273 DE 2009, habeas data y demás normativa aplicable.

8.15.15 Política de uso del correo electrónico

8.15.15.1 Uso del correo personal

El uso de cuentas de correo personales, basadas en acceso a web, tipo Gmail, hotmail, yahoo, podrán ser utilizados con moderación, bajo las siguientes condiciones:

El acceso deberá ser exclusivamente a aquellos correos que sean de plena confianza, y en ningún caso deben abrirse enlaces o descargarse ficheros adjuntos en el ordenador

del usuario o de otros usuarios, aunque provengan de personas conocidas, para evitar así la intrusión de virus o códigos maliciosos.

> Es indebido el reenvío de información clasificada, confidencial y reservada a cuentas de correo electrónico personales o que no se encuentren bajo control directo de la institución.

- **8.15.15.2 USO DE CORREO INSTITUCIONAL**

El correo electrónico institucional, las listas de distribución, los contactos, los servicios de mensajería instantánea y demás servicios de comunicación electrónica, son herramientas cuyo objetivo principal es facilitar la comunicación corporativa exclusivamente en el ámbito laboral.

Las partes acuerdan que la utilización de los servicios de comunicación y difusión de la información quedará sujeta a las siguientes condiciones:

No se debe utilizar las herramientas de comunicación para uso personal. asimismo, se prohíbe el envío de correo electrónico con mensajes ofensivos, amenazantes, contenido ilícito o fraudulento.

No se permite el uso de correo electrónico con fines lucrativos o comerciales, para uso recreativo o cualquier otro que no guarde relación con la actividad laboral.

No se permite el uso del correo institucional para la inscripción a “newsletter”, grupos de noticias, o similares que no estén directamente relacionadas con la actividad profesional desarrollada por el usuario y que resulten de plena confianza.

Las listas de distribución de correo solo podrán ser utilizadas para los fines propios del cuerpo de Bomberos de Bucaramanga, y nunca con fines publicitarios, comerciales o de índole personal que no vayan relacionadas con actividades propias del desempeño laboral.

No se debe acceder sin autorización a las comunicaciones que circulan por la red, así como su manipulación, destrucción y apropiación indebida.

8.15.15.3 Política de uso de internet

Bomberos de Bucaramanga permite el acceso a los servicios de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios, evitando el uso inadecuado de la información en las aplicaciones WEB.

La navegación por Internet utilizará un software adecuado para filtrar los accesos a los sitios que a consideración del encargado de sistemas sean inapropiados para la institución, o innecesarios para la actividad laboral.

La navegación por sitios web, el envío de mensajes, registros, altas, relleno de formularios y cualquier otra actividad realizada vía Internet, serán completa responsabilidad del

usuario emisor y en todo caso deberá asumir las consecuencias que emanen de su actuación.

No se permite la navegación a sitios con contenidos ilícitos, material pornográfico, terrorismo, hacktivismo, de contenido racista, sexual, o cualquier material que atente contra la dignidad y los principios morales.

La descarga de archivos de internet debe ser con propósitos laborales y de forma que no afecte el servicio.

8.15.15.4 Política del uso de herramientas y redes p2p

No se permite la instalación de programas P2P (peer to peer), o cualquier otra aplicación para el intercambio de archivos que saturen el ancho de banda de la conexión a Internet, impidiendo el acceso a los demás usuarios o entorpeciendo las conexiones a la Red.

8.15.15.5 Restricciones y política de uso de software de mensajería instantánea y redes sociales.

No se podrá instalar ningún software de servicio telemático o de mensajería instantánea sin autorización expresa del personal directivo, o del administrador de sistemas en su caso.

No se permite utilizar lenguaje obsceno, agresivo, ofensivo o discriminatorio en el envío de comunicaciones a través de servicios de mensajería instantánea.

Por seguridad, no se deberán descargar por ningún motivo ficheros adjuntos provenientes de remitentes desconocidos.

No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la entidad.

El usuario será responsable de todo daño ocasionado en los equipos informáticos y sistemas de información, por negligencia, violación, o mal uso de los servicios de mensajería instantánea.

8.15.15.6 Programas y dispositivos de control y monitorización

El administrador de sistemas pondrá en funcionamiento herramientas de control automatizadas para analizar y detectar los usos y comportamientos indebidos o ilícitos en la red, no implicado dicho control violación a la privacidad o a la intimidad de los usuarios.

Las partes acuerdan que por cuestiones de seguridad toda la información que circula por la red, así como por el correo electrónico de las cuentas administradas por la institución, podrá ser monitoreada y sujeta a controles y reportes sobre su uso, brindando información como: usuario, fecha de accesos, hora de accesos, bytes transferidos, almacenamiento

de ficheros, acceso a los servidores, sitios visitados, tiempo de navegación por la red, entre otros.

8.15.15 7 Política de uso de equipos informáticos fuera de la institución

Las entradas y salidas de los equipos informáticos necesarios para el desarrollo de las actividades de la institución, serán autorizadas por el responsable de seguridad.

El usuario queda obligado a realizar la petición motivada por escrito, indicando el equipo a utilizar fuera de la institución, fecha de salida y fecha prevista de entrega, quedando obligado el responsable de seguridad a responder por escrito a la petición.

El responsable de seguridad implementará las medidas necesarias para garantizar la integridad y seguridad de los equipos informáticos fuera de la institución, así como de mantener un registro actualizado de las entradas y salidas de los mismos.

8.15.15.8 Uso de licencias de software

Los usuarios están obligados a respetar las condiciones de licencia y copyright del software instalado en los equipos informáticos, siendo responsables de su adecuada utilización.

Todo software protegido por copyright no podrá ser copiado, ni se podrá disponer de cualquier información protegida por los derechos de autor que esté en formato electrónico en el equipo de cualquiera de los usuarios.

Los usuarios serán responsables de todo software instalado en sus equipos sin autorización expresa del administrador de sistemas, así como de uso y en su caso, de los daños que causen a los equipos o sistemas de información que deriven de su uso o instalación.

Cualquier actividad que infrinja las leyes de la propiedad intelectual, incluyendo los derechos de autor, marcas o derechos registrados y el de su reproducción será sancionado por la normativa.

8.15.15. 9 consecuencias derivadas del mal uso de los medios o recursos tecnológicos

Los usuarios se comprometen a colaborar con el administrador de sistemas para llevar a cabo toda investigación que tenga por objeto encontrar las posibles causas derivadas del mal uso de los recursos tecnológicos.

Toda incidencia detectada en los equipos informáticos, así como en los sistemas de información, podrán derivar en la suspensión o restricción del acceso o uso de los servicios al usuario, así como la aplicación de las medidas que el Director General, considere oportunas al incumplimiento de lo establecido en el presente documento.

8.15.15.10 Política para realización de copias de seguridad de trabajo.

Asegurar la operación de realización de copias de información en puestos de trabajo de usuario final.

Las copias de seguridad es una réplica de la información más importante de la entidad el cual se debe realizar para salvaguardarla en caso de pérdida por intrusos, virus, desastres naturales etc. Para mantener las copias de seguridad bajo los principios básicos de la seguridad que son la integridad, la confidencialidad y el control de acceso, se deben crear procesos minimizar el riesgo de perder la integridad de la información:

- Asignar una persona responsable para el almacenamiento, el cual mantenga la integridad de las copias de seguridad que se encuentran en su custodia el cual ayude a crear una protección más eficaz de la información sensible de la entidad.

- Las copias de seguridad se deben realizar en dispositivos externos al servidor.

- Las copias de seguridad se deben programar con el usuario para realizarlas en el tiempo que no se está manipulando la información.

8.15.15.11 Política de protección física de equipos y servidores

Los equipos de cómputos y servidores de la entidad son un activo importante para la realización de los procesos internos, permitiendo una buena y oportuna prestación del servició a los clientes que lo requieren, por ende, se deben realizar procedimientos que permita el buen funcionamiento, el cual se recomiendan los siguientes:

- Realizar mantenimiento preventivo a los equipos mínimo dos veces al año, para evitar daños en los componentes por el polvo que se almacena, el cual no permite un adecuado enfriamiento de los componentes, acortando la vida útil del equipo.

- evitar fumar cerca a los equipos debido a que la ceniza del cigarro contiene elementos químicos causando corrosión a los componentes internos de la computadora.

- Realizar monitoreos constantes de rendimiento al servidor para diagnosticar errores que se generen de software.

- Desfragmentar el disco duro para eliminar archivos temporales o archivos innecesarios, debido a que consume recursos en los equipos de cómputo.

- Mantener los equipos en lugares refrigerados para evitar recalentamiento en los componentes de cada uno de los quipos de computo.

- Mantener un extintor que cumpla en caso de incendio para poder mitigar daños en el centro de datos de la entidad.

8.15.15.12 Políticas para funciones y responsabilidades de ingenieros y/o técnicos de soporte.

Los ingenieros y/o técnicos de soporte tendrán las siguientes funciones y responsabilidades:

8.15.15.13 Funciones

- Brindar apoyo a los usuarios a los usuarios a problemas presentados por software o hardware.
- Resolver cualquier problema técnico que presenten los equipos de cómputo.
- Configurar las impresoras o dispositivos de hardware.
- Crear direccionamientos ips para equipos nuevos que se conecten al dominio.
- Monitorear los procesos en los servidores y los espacios en discos duros.
- Realizar inventario de software y hardware existente en la entidad.
- Asesorar en compra de productos y servicios de tecnología, realizando un análisis técnico de la propuesta.

8.15.15.14 Responsabilidad

- Utilizar los recursos asignados eficientemente manteniéndolos en buen estado.
- Utilizar, mantener en cadena de custodia la confidencialidad de la información que le asigna Bomberos de Bucaramanga.
- Cumplir con las normas del sistema de gestión de calidad de Bomberos de Bucaramanga.
- Podrán ingresar remotamente a los equipos de cómputo exclusivamente para solucionar problemas expuestos por el usuario del equipo.
- Auditar periódicamente, sin previo aviso los sistemas y servicios de la red, para revisar la existencia de cualquier archivo no autorizado, configuraciones que no corresponden a las de la entidad, permisos que pongan en riesgo la seguridad de la información confidencial de Bomberos de Bucaramanga.
- Reportar a Bomberos de Bucaramanga cualquier incidente de violación de la seguridad en la entidad.
- Mantener actualizados los sistemas de los equipos de cómputo de Bomberos de Bucaramanga.

8.15.15.15 Responsabilidades y deberes para los usuarios

Los usuarios tendrán las siguientes responsabilidades y deberes con Bomberos de Bucaramanga.

- Todos los usuarios son responsables de la actividad en el uso del acceso autorizado al sistema.
- Los usuarios y contraseñas son únicos para cada usuario el cual deben mantener en secreto para la autenticación en el sistema.
- Cualquier usuario que sospeche del acceso no autorizado y que este en uso por otra persona, se debe reportar al administrador de sistemas para que realice el cambio de contraseña inmediatamente.
- El usuario únicamente debe realizar el cambio de contraseña cuando el sistema lo solicite.
- El usuario debe mantener confidencialidad con la información asignada por Bomberos de Bucaramanga.

- El usuario debe evitar el uso de recursos no relacionados con las actividades interpuestas en el objeto contractual del contrato.
- El usuario no debe instalar programas virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico que causen cualquier tipo de alteración o daño en los recursos de Bomberos de Bucaramanga.
- El usuario no debe albergar datos de carácter personal en ninguna de las unidades locales del equipo de cómputo.

8.15.15.16 Uso y administración de recursos informáticos (hardware)

- El equipo de cómputo instalado en las diferentes áreas de Bomberos de Bucaramanga sólo podrá ser utilizado por el personal de Bomberos de Bucaramanga, el cual lo utilizará para el desarrollo de sus funciones institucionales, con la finalidad de garantizar la compatibilidad, estandarización e integridad de los recursos informáticos.
- La instalación y reubicación de equipos de cómputo, estará a cargo del personal que designe la Dirección General.
- Los equipos sólo podrán ser abiertos para su revisión, configuración o reparación, por el personal autorizado por la Dirección General o Dirección Administrativa.
- El usuario será responsable de vigilar que el equipo de cómputo asignado (Equipo Portátil, Equipo de escritorio o impresora) quede debidamente apagado, cuando no esté en uso.
- En caso de retiro definitivo de personal o reasignación del equipo de cómputo, el jefe del área deberá notificar al centro de soporte, para configurar las novedades, accesos, cancelaciones.
- Para cada equipo de cómputo conectado a la red de la entidad, la Dirección General establecerá las herramientas (hardware y/o Software) necesarias para implementar los controles establecidos en esta política, mantener el inventario de recursos informáticos y monitorear el uso adecuado de los equipos de cómputo.
- Solamente el personal del centro de soporte está encargado de que todos los equipos de Bomberos de Bucaramanga estén conectados en red y afiliados al dominio.

- Los empleados no pueden modificar la configuración del equipo de cómputo asignado (cambiar, instalar y/o retirar partes).

8.15.15.17 Uso y administración de recursos informáticos (software)

- Los programas o paquetes utilizados en Bomberos de Bucaramanga, serán suministrados única y exclusivamente por el área de Telemática, quien controla y resguarda las licencias originales de uso de software instalado en dicho equipo.
- Toda necesidad de instalación de software deberá ser notificada al área de telemática, quién comprobará la procedencia lícita y llevará a cabo el proceso de instalación. En caso de una auditoria informática, el usuario será el único responsable del software que no esté autorizado, y que esté instalado en el equipo.
- Los usuarios de equipo de cómputo deberán respetar y hacer respetar las leyes, normas y lineamientos establecidos, como la Ley de derechos de Autor, Leyes de

derechos reservados (copyright), Leyes de patentes y las condiciones de licenciamiento de cada software.

- Queda prohibida la instalación y/uso de programas y aplicaciones cuyo propósito no esté relacionado con las actividades que desarrolle Bomberos de Bucaramanga, así como instalar en las computadoras juegos, programas de música, participaciones en redes sociales, chats, o programas de cómputo que no cuenten con licencia autorizada por el área de telemática. Su cumplimiento será responsabilidad de cada usuario.
- En caso de que existan dudas sobre los programas autorizados o indebidamente instalados, el área de telemática, proporcionará necesario para informar las dudas al respecto, o para desinstalar los programas que el usuario solicite.
- Si se requiere adquirir programas específicos (software) que contribuyan a mejorar el rendimiento de las actividades diarias en Bomberos de Bucaramanga, deberán solicitarla al área de telemática para que en conjunto con la Dirección administrativa y Dirección General se evalúe, analice y se autorice la adquisición del mismo.
- Los funcionarios no deben destruir, copiar o distribuir los archivos de la entidad sin los debidos permisos.
- Los funcionarios no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la entidad en busca de información de otros sin su autorización o introducir intencionalmente software para causar daño o impedir el normal funcionamiento de los sistemas.
- Queda totalmente prohibido cualquier copia de los programas, paquetes o sistemas instalados en los equipos, por personal que no esté autorizado por la Dirección Administrativa y Financiera o la Dirección General.
- Los funcionarios no deben suministrar ninguna información de la entidad a entes externos sin las autorizaciones respectivas esto incluye los controles que se utilizan en los sistemas de información y su respectiva implementación.

- Los usuarios deben informar inmediatamente al área de telemática toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos e intentos intromisión y no deben distribuir esta información interna o externamente.
- Todo funcionario que utilice los recursos de los sistemas, tiene la responsabilidad de velar por el buen nombre de la empresa, la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

8.15.15.18 Responsabilidades derivadas del incumplimiento de la política

El presente documento estará regulado por las leyes y normativas colombianas, en relación con protección de datos de carácter personal, propiedad intelectual y uso de herramientas telemáticas, así como la normativa aplicable dentro del ámbito laboral y toda la que pueda aparecer en un futuro.

8.15.15.19 Medios electrónicos disponibles

8.15.15.19 Dominio oficial-Bomberosdebucaramanga.gov.co

Este dominio estará bajo administración y gestión exclusiva de la entidad. Los cambios en registros DNS, y demás serán autorizados y realizados exclusivamente por la entidad a través de las cuentas de usuario con la entidad de registro del mismo.

8.15.15.20 Sitio web

La página oficial de BOMBEROS DE BUCARAMANGA está disponible en el vínculo www.bomberosdebucaramanga.gov.co, en ella se encuentra disponible la publicación de la información administrativa, informes de gestión, legal, portafolio de servicios, noticias de la entidad. Para la publicación de información en la página WEB el líder de cada área debe solicitar mediante comunicación ya sea escrita, correo electrónico o telefónica a la oficina de Sistemas, la solicitud de publicación en la página web de la información correspondiente a su área.

8.15.15.21 Redes sociales

Las páginas oficiales de Bomberos de Bucaramanga en las redes sociales, permiten una interacción más amigable y cercana con la comunidad de Bucaramanga; las cuales se encuentran disponibles para interactuar con los usuarios, en los siguientes enlaces:

- Página oficial de Facebook https://www.facebook.com/bomberos.debucaramanga
- Cuenta twitter https://twitter.com/BomberosBGA

8.16 ESTRATEGÍA N° 2. TOMA DE DECISIPNES ESTRATÉGICAS A PARTIR DE ANALISIS DE DATOS-OPEN DATA

La toma de decisiones estratégicas soportada en el análisis de datos o estadísticas, data desde la segunda guerra mundial. Dado lo anterior es pertinente decir, que, disponer de información actualizada y de calidad puede aportar grandes ventajas a la hora de tomar decisiones y detectar debilidades o fortalezas en los procesos que pueden conducir a oportunidades de mejora. Si bien es cierto que las estadísticas son datos numéricos que si no son utilizados como fuente de información para la mejora podrían pasar a formar parte de un archivo sin importancia.

En Bomberos de Bucaramanga, se encuentran y se guardan importantísimos datos que son recolectados en el **sistema de Gestión de Operaciones como fuente de información,** durante la gestión de la prestación del servicio misional, sin embargo, estos datos no son aplicados para la toma de decisiones, a la hora de implementar estrategias que contribuyan al mejoramiento de la prestación del servicio esencial de prevención, seguridad y atención integral del riesgo contra incendio en la comunidad de Bucaramanga o donde se requiera.

Para Bomberos de Bucaramanga, por ejemplo, si en los datos estadísticos se evidencia que el incremento de los incendios forestales son provocados en la misma época del año por la misma causa, se debería tomar los datos estadísticos que evidencian la variación para este caso y con ellos formular una estrategia para mitigar la causa que incrementan estos incendios forestales.

Otro punto a tener en cuenta es que los mismos datos se pueden analizar de distintas formas, combinando las probabilidades de riesgos de incendio, las probabilidades de rescates exitosos, las causas generadoras de los eventos y con toda esta información formular estrategias desde el área de Prevención.

Otro aspecto a tener en cuenta es el equilibrio entre el análisis de los datos que realiza quien reporta la información en este caso es el área de Operaciones y la necesidad de información de quien analiza los datos estadísticos para la formulación de la estrategia, es decir, el área de Prevención; porque lógicamente, el analista quiere disponer de mucha información; sin embargo la información que está puesta como dato plano requiere de mayor esfuerzo en tiempo y en análisis, entendiendo que cualquier gestión basada en el papel siempre será más larga y tendrá mayores probabilidades de errores que si la misma tarea se realiza de manera automatizada.

Es por ello que una opción interesante y efectiva para la toma de decisiones estratégicas basada en Datos estadísticos o a partir de Análisis de Datos la mejor opción es utilizar una herramienta digital que automatice los reportes, que pueda jugar con las diferentes opciones de combinar las variables que hará del proceso una estrategia exitosa y optimice los recursos.
Finalmente, la importancia de disponer de un historial de los datos que pueden ser analizados, y mediante una herramienta tecnológica poder de manera efectiva definir tendencias, ver los efectos realizados en la gestión, determinar cuáles son las debilidades de los procesos, las fortalezas y a partir de ellos construir una estrategia o una oportunidad de mejora para Bomberos de Bucaramanga y tal vez con esta información aplicada en fortaleza salvar muchas vidas.

8.16.1 Gestión del riesgo TI Bomberos de Bucaramanga

La gestión del riesgo para TI en la entidad debe incluir entre otras las siguientes variables y probabilidades:

1. Identificación de vulnerabilidades y amenazas sobre los activos de información.
2. Identificación de Riesgos, Evaluación de Riesgos
3. Monitoreo
4. Planes de Acción

8.16.2 Política de administración del riesgo- Bomberos de Bucaramanga

En cumplimiento de su función misional: Garantizar la Protección de las vidas y el Patrimonio de los Ciudadanos; Identifica, Valora y controla los Riesgos de los Procesos y de la corrupción; mediante la ejecución de sus Procesos; asegurando la Prestación de sus servicios de manera transparente y eficiente; administrando, reduciendo, evitando o transfiriendo situaciones de riesgos que puedan afectar el logro de los objetivos Institucionales". El objetivo de la política es Identificar los Riesgos de corrupción en los procesos de la Entidad que puedan afectar el cumplimiento de los objetivos Institucionales, la seguridad y el bienestar de los servidores públicos y el manejo adecuado de los recursos.

La política de Administración del Riesgo es aplicable a todos los procesos, proyectos, planes y programas de la entidad y a todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones.

8.16.3 Contexto del riesgo

8.16.3.1 Matrices de riesgo, análisis estratégico

Antes de iniciar cualquier identificación de riesgos, es necesario estudiar el contexto del riesgo, el cual sirve para identificar las fuentes que pueden dar origen a los riesgos; este contexto incluye: el contexto estratégico, los proyectos de inversión, los procesos y los servicios misionales de Bomberos de Bucaramanga, identificando los factores a considerar a la hora de identificar los riesgos. Así mismo, es necesario tener en cuenta los requisitos legales que pueden intervenir asociados con los elementos mencionados, así como otros elementos adicionales como son PQRSD, interpuestas por la ciudadanía por causas inherentes a la prestación del servicio de la entidad. Para la definición del contexto del riesgo se deben contemplar los siguientes aspectos (Ver Gráfico 2: Contexto del riesgo):

PROCESO	**TECNOLOGIA DE INFORMACION Y COMUNICACION**
AREA	**DIRECCIÓN ADMINISTRATATIVA Y FINANCIERA**
CONTEXTO EXTERNO	Para el proceso de Gestión de la Tecnología e Información se contemplaron dentro de la matriz de riesgos -Contexto estratégico los siguientes factores: 1.**POLÍTICOS**: Cambios de gobierno, Legislación, Políticas públicas, regulación. **2. TECNOLÓGICOS:** Nuevas tecnologías, acceso a Sistemas de información externos, gobierno en línea. **3. ARTICULACIÓN INTERINSTITUCIONA**L: Relación con otras entidades públicas **Políticos**: De acuerdo con las normativas y Legislación en temas relacionados con uso de Tecnología, las cuales establecen lineamientos que las entidades públicas deben implementar dentro de su operación y gestión. Adicionalmente la normatividad específica que aplica a los procesos misionales y administrativos de Bomberos de Bucaramanga, que requiere en algunos casos la implementación de soluciones de tecnología. **Tecnológicos:** Nuevas tecnologías de la Información implementadas que requieren ser actualizadas en la entidad para permitir la interacción con otras entidades. **Articulación interinstitucional:** El objetivo general al elaborar el PETI es la búsqueda de la articulación de la gestión de los procesos, la prestación del servicio misional con la tecnología, así como con las entidades del estado que se requiera, con el fin de facilitar los trámites y servicios que presta la entidad, lograr la interacción con una ciudadanía participativa, que en ocasiones cuenta con un componente tecnológico superior al existente en la entidad.

PROCESO	**TECNOLOGIA DE INFORMACION Y COMUNICACION**
AREA	**DIRECCIÓN ADMINISTRATATIVA Y FINANCIERA**
CONTEXTO INTERNO	Para el proceso de Gestión de la Tecnología e Información se contemplaron dentro de la matriz de riesgos los siguientes factores: **FINANCIEROS:** Presupuesto General Bomberos, Asignación de Recursos, Proyectos TI incluidos en el Plan de Anual de Adquisiciones. **TALENTO HUMANO:** Personal capacitado en TI, disponibilidad de personal, Política de Seguridad y Salud en el Trabajo. **TECNOLOGIA:** Plataforma tecnológica robusta, Disponibilidad de Datos, Sistemas de Información implementados. **ESTRATÉGICOS:** Planeación Institucional, Direccionamiento estratégico, Trabajo en equipo, Liderazgo. Financieros: Proyectos de Inversión, Adquisición e implementación de soluciones TIC, condicionada a la posible asignación presupuestal que anualmente se realice al Procesos de Gestión de la Tecnología e Información, mediante el Plan Anual de Adquisiciones en el rubro 22152 Plan de Sistematización. **Tecnología:** La entidad debe actualizar y modernizar su plataforma tecnológica; aún persisten procesos que se desarrollan de manera operativa, un solo ejemplo claro es el Proceso de Gestión Documental, los Sistemas de Información existentes no son actualizados ni mantenidos como es el caso del sistema administrativo y contable que es fundamental para la operación debido a que los procesos administrativos como Nómina, contabilidad, Almacén, Recursos Físicos entre otros están soportados en este sistema de Información, falta capacitación en el uso adecuado de las pocas herramientas y elementos tecnológicos existentes. **Estratégicos:** Teniendo en cuenta que el Proceso TIC a partir de MIPG, es un proceso transversal que impacta a todos los procesos, la elaboración e implementación del Plan Estratégico de Tecnologías de la Información PETI, es la estrategia adecuada para buscar una mayor alineación y mejora Institucional entre los procesos y las soluciones tecnológicas que apoyen la prestación del servicio esencial y a las áreas administrativas que son procesos de apoyo al cumplimiento de la misión Institucional. **Talento humano:** Teniendo en cuenta que la entidad debe iniciar el proceso de desarrollo en TI, como una propuesta de revolución digital y tecnología, que a partir del PETI, MIPG y al incorporar a Talento Humano, así como a Tecnologías de la Información como ejes transversales a todos los procesos; la prestación de los servicios de tecnología, requiere contar con personal competente, innovador y especializado en el área, de acuerdo con los requerimientos exigidos por la entidad. MIPG concibe al talento humano como el activo más importante con el que cuentan las entidades y, por lo tanto, como el gran factor crítico de éxito que les facilita la gestión y el logro de sus objetivos y resultados, es por ello, que se encuentra como la Primera Dimensión de las siete con las cuales se implementa MIPG. Con esta dimensión, y la implementación de las políticas que la integran, se logra cumplir con el objetivo central de MIPG “Fortalecer el liderazgo y el talento humano bajo los principios de integridad y legalidad, como motores de la generación de resultados de las entidades públicas”.

Tabla No. 10 Matriz de Riesgo Análisis Estratégico del proceso TIC.

8.16.3.2 Contexto del proceso tecnologías de la información y comunicación

PROCESO	**TECNOLOGIA DE LA INFORMACION Y COMUNICACION**
AREA	**DIRECCION ADMINISTRATIVA Y FINANCIERA**
CONTEXTO DEL PROCESO	**CONTEXTO DEL PROCESO** 1. **PROCESOS DINÁMICOS – INTERACCIÓN** **2. TRANSVERSALIDAD.** **4. PROCEDIMIENTOS ASOCIADOS.** **5. RESPONSABLES DEL PROCESO.** **6. CAPACIDAD.** **8. GESTIÓN DEL CONOCIMIENTO.**
	Para el proceso de Gestión de la Tecnología e Información se contemplaron dentro de la matriz de riesgos los siguientes factores: **Procesos Dinámicos -Interacción:** El proceso TI, en Bomberos de Bucaramanga, interactúa con los demás procesos por medio de la entrega de servicios de soluciones tecnológicas, soporte técnico y asesoría en Sistemas de Información, en herramientas tecnológicas (telefonía, correo, comunicaciones, conectividad, infraestructura, licenciamiento, entre otros), que apoyan los procesos misionales y administrativos. **Transversalidad:** MIPG define la Información y Comunicación como una dimensión articuladora de las demás, puesto que permite a las entidades vincularse con su entorno y facilitar la ejecución de sus operaciones a través de todo el ciclo de gestión. La quinta dimensión de MIPG -Comunicación e Información-, tiene como propósito garantizar un adecuado flujo de información interna, es decir, es aquella que permite la operación interna de una entidad, así como de la información externa, esto es, aquella que le permite una interacción con los ciudadanos; para tales fines se requiere contar con canales de comunicación acordes con las capacidades organizacionales y con lo previsto en la Ley de Transparencia y Acceso a la Información. *(Tomado de Dimensión 6 MIPG).* **Infraestructura TI:** La capacidad instalada de TI para atender los requerimientos de los usuarios internos y externos es inferior, por lo tanto, requiere robustecer la plataforma tecnológica así como fortalecer el equipo humano de sistemas, debido a que solo existe una Ing. de sistemas para soportar todos los requerimientos tanto de las áreas administrativas como los procesos misionales, que podría impactar el cumplimiento de los objetivos Institucionales al materializarse los riesgos de TI, por falta de controles para la mitigación de las causas que generan los riesgos. **Procedimientos asociados y responsables del proceso:** De acuerdo con la propuesta de mapa de procesos, que la entidad debe implementar a partir del primer trimestre de 2019, se plantea la articulación del Proceso de Gestión de Tecnología y comunicaciones con MIPG, siendo transversal a todos los procesos y procedimientos, por tal razón será un proceso con la perspectiva de que las TIC son un marco de referencia para que la gestión en los procesos se desarrollen de manera más dinámica, al interactuar articuladamente con otros; es así que al elaborar el Plan Estratégico de Información y comunicaciones de Bomberos de Bucaramanga, precisa la necesidad de documentar los procedimientos que conlleven a preservar, proteger la información de la entidad. **Gestión del conocimiento:** En el sector público se genera una cantidad importante de datos, información, ideas, investigaciones y experiencias que, en conjunto, se transforman en conocimiento. Este debe

	estar disponible para todos, con procesos de búsqueda y aplicación efectivos, que consoliden y enriquezcan la gestión institucional. La actual era digital o de la información le plantea al Estado retos de cambio y de adaptación para mejorar la atención de las necesidades de los ciudadanos quienes exigen respuestas más rápidas y efectivas para la garantía de sus derechos. La Gestión del Conocimiento y la Innovación fortalece de forma transversal a las demás dimensiones en cuanto a que el conocimiento que se genera o produce en una entidad es clave para su aprendizaje y su evolución. (Tomado de Dimensión 6 MIPG).

Tabla No. 11 Contexto del Riesgo.

8.16.3.3 Elementos para construir la matriz del riesgo TI

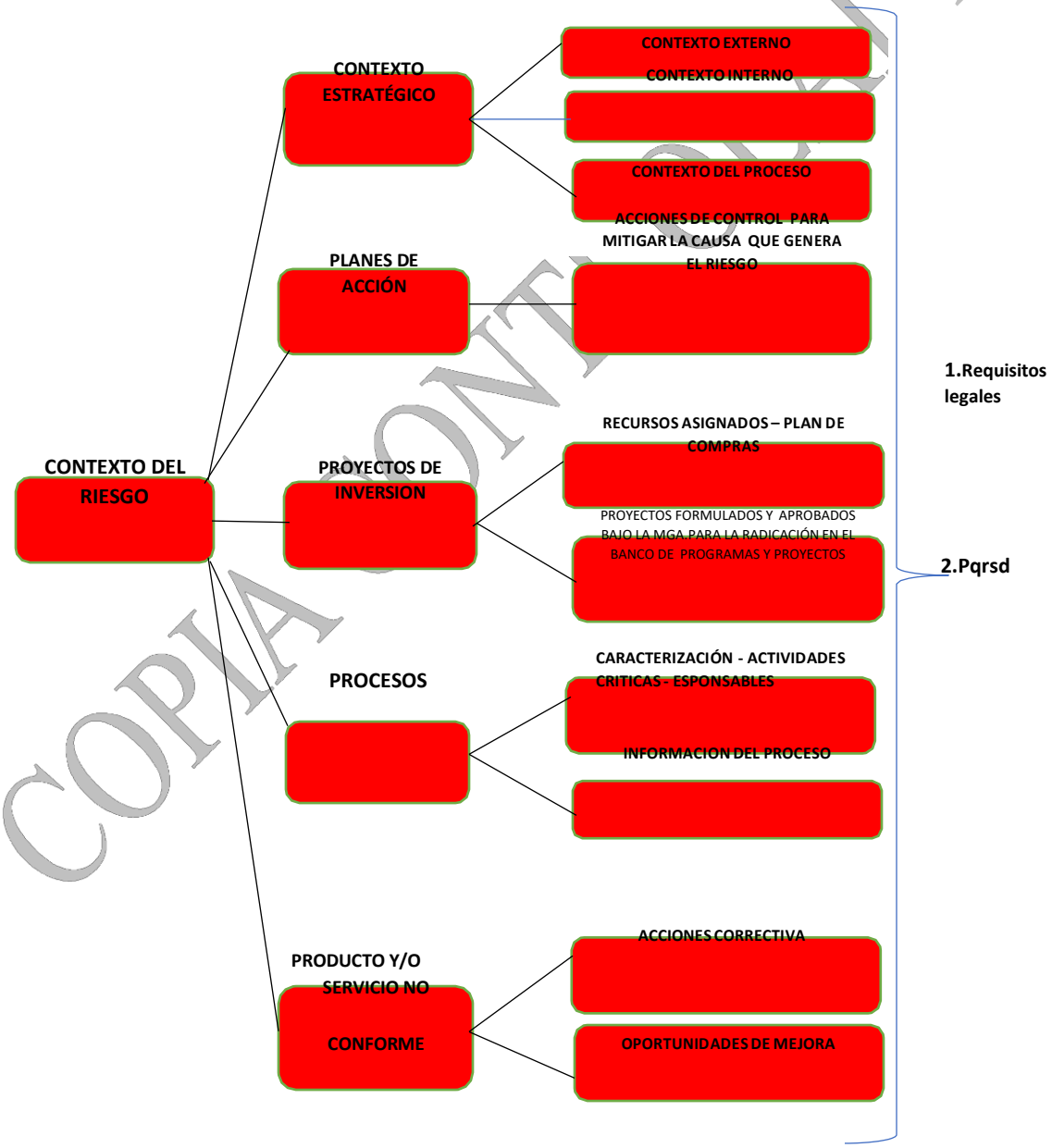


Ilustración No. 2 Elementos para construir Matriz del Riesgo

9. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Creación del documento	2018/12/19
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, se modifica el cronograma de actividades.	Agosto 26 de 2020
2.0	Se actualiza el plan según las necesidades de la vigencia 2022.	Enero 2022