

**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

Fecha: Enero /2023

Versión: 3

Aprobado por: Asesor SST

Autorizado por: Comandante Operativo

Página 1 de 2

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.**1. OBJETIVO**

Generar conciencia sobre las responsabilidades en el uso de los equipos informáticos, tecnológicos y de comunicación y de la información disponible.

2. ALCANCE

Este instructivo es para todo el personal que dispone de acceso a la información física y digital en las Instalaciones del **CUERPO DE BOMBEROS VOLUNTARIOS DEL MUNICIPIO DE RIVERA – HUILA**, incluyendo el uso de los equipos informáticos, tecnológicos y de comunicación.

3. DIRECTRIZ DE USO

1. La responsabilidad por la seguridad de la información no es únicamente de Sistemas, es un deber de cada Unidad Bomberil.
2. Los mecanismos de acceso que les sean otorgados a las Unidades Bomberiles (clave de red y correo) son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.
3. Las Unidades Bomberiles son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
4. Las Unidades Bomberiles deben informar inmediatamente al área de sistemas toda vulnerabilidad física y lógica encontrada en los sistemas, aparición de virus, programas sospechosos e intentos de intromisión o el mal funcionamiento del equipo y no deben distribuir este tipo de información interna o externamente.
5. Las Unidades Bomberiles no deben instalar software en sus computadores sin la debida autorización del Comandante Operativo.
6. Las Unidades Bomberiles no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la Institución en busca de archivos de otros sin su autorización.
7. No deben introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas, en caso que esto ocurra el Comandante tomará las medidas necesarias y correspondientes de acuerdo a lo establecido entre los contratos laborales y legislación bomberil colombiana existente.
8. Las Unidades Bomberiles no deben suministrar información de la Institución a ningún ente externo sin las autorizaciones respectivas esto incluye los controles del sistema de información y su respectiva implementación.
9. Las Unidades Bomberiles no deben destruir, copiar o distribuir los archivos de la Institución sin los permisos respectivos.
10. Toda Unidad Bomberil que utilice los recursos de los Sistemas, tiene la responsabilidad



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fecha: Enero /2023

Versión: 3

Aprobado por: Asesor SST

Autorizado por: Comandante Operativo

Página 2 de 2

de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, toda la información deberá ser tomada como crítica lo cual implica la NO divulgación a entes externos.

11. Los computadores, sistemas y otros equipos deben usarse solamente para las actividades propias de la Institución, por lo tanto las Unidades Bomberiles no deben usar sus equipos para asuntos personales a menos que exista una autorización respectiva que evalúe el riesgo informático de tal labor.
12. Todos los datos de propiedad de la Institución se deben clasificar dentro de las siguientes categorías para los datos sensibles: SECRETO, CONFIDENCIAL, PRIVADO, y para los datos no sensibles la categoría es PÚBLICO.
13. Cualquier tipo de información interna de la Institución no debe ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al de la Institución y se debe cumplir con los procedimientos de autorización internos para los casos en que se requiera, en caso tal que ocurra lo anteriormente mencionado acarreará las respectivas sanciones de acuerdo al contrato laboral y a leyes de protección de datos vigentes según la legislación colombiana.
14. Todos los errores cometidos por las Unidades Bomberiles de la Institución y que son detectados, deben cumplir con un proceso de investigación de acuerdo con los procedimientos y tiempos establecido de acuerdo al contrato y reglamento interno.
15. Los equipos de cómputo de la Institución no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del Comandante Operativo.
16. Las Unidades Bomberiles deben reportar al Comandante Operativo, sobre daños o pérdida del equipo que tengan a su cuidado y sea propiedad de la Institución.
17. Al terminar la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de la Institución. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

Dado en el Municipio de Rivera – Huila, a los 5 días del mes de Enero de 2023, en las Instalaciones de la Estación Central del Cuerpo de Bomberos Voluntarios del Municipio de Rivera – Huila.

En constancia y para efectos legales, firma;


ET. EDIDSON FERNANDEZ
Comandante Operativo
Firma Representante Legal



**Cuerpo de Bomberos
Voluntarios de Rivera
Comandante**