E.S.P
Nit 816.001.463-1
Calidad y eficiencia a su servicio

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

## EMPRESA DE SERVICIOS PÚBLICOS DE MISTRATÓ

## VIGENCIA 2025

CONTENIDO

## INTRODUCCIÓN

El sistema computacional utilizado para el manejo de la información relevante contenida en el computador principal de facturación y los diferentes ordenadores empleados por los funcionarios de la Empresa de Servicios Públicos de Mistrató, se encuentra expuesto a una serie de riesgos inherentes que, de no ser gestionados adecuadamente, podrían generar problemas significativos. Estos riesgos no solo involucran fallos técnicos, sino también factores humanos y ambientales que pueden comprometer tanto el software como el hardware de la empresa. Los equipos informáticos y las aplicaciones utilizadas por los empleados están sujetos a amenazas que provienen de diversas fuentes, tales como errores humanos, ciberataques, y condiciones del entorno que pueden afectar su funcionamiento de manera negativa.

Adicionalmente, un factor que debe ser considerado es la obsolescencia tecnológica de los equipos. Con el paso del tiempo, tanto el hardware como el software de los sistemas tienden a perder eficiencia, lo que puede generar vulnerabilidades adicionales y dificultades operativas. La falta de actualizaciones y la incompatibilidad con nuevas tecnologías son riesgos potenciales que pueden afectar la estabilidad y la seguridad de los sistemas.

En este contexto, es fundamental que la Empresa de Servicios Públicos de Mistrató implemente un plan de seguridad integral que garantice la protección adecuada de la información que maneja. Este plan debe contemplar no solo medidas para proteger los datos sensibles contra accesos no autorizados o pérdidas, sino también estrategias para asegurar la privacidad de la información de los usuarios y la continuidad de los servicios en caso de contingencias tecnológicas. La correcta custodia de la información es un elemento esencial para el funcionamiento eficiente y seguro de la empresa, por lo que resulta imprescindible adoptar protocolos y herramientas que resguarden la integridad de los datos gestionados en todos los niveles.

## OBJETIVO GENERAL

Desarrollar e implementar un plan de seguridad integral para la Empresa de Servicios Públicos de Mistrató, que permita gestionar adecuadamente los riesgos inherentes al manejo de la información, protegiendo los equipos informáticos, las aplicaciones y los datos sensibles, garantizando la estabilidad, la seguridad y la continuidad de los servicios.

## OBJETIVOS ESPECÍFICOS

- Identificar y evaluar los riesgos tecnológicos, humanos y ambientales que afectan a los equipos informáticos, el software y la seguridad de la información en la Empresa de Servicios Públicos de Mistrató.

- Proponer estrategias de mitigación para prevenir ciberataques, errores humanos y fallos técnicos que puedan comprometer el funcionamiento de los sistemas informáticos de la empresa.

- Establecer protocolos de actualización y mantenimiento para los equipos y aplicaciones, a fin de reducir la obsolescencia tecnológica y garantizar la compatibilidad con nuevas tecnologías.

- Implementar un plan de continuidad de servicios, que contemple acciones específicas ante contingencias tecnológicas, asegurando el funcionamiento ininterrumpido de la empresa.

## ALCANCE

La política de Seguridad de la Información aplica para todos los funcionarios de la Empresa de Servicios Públicos de Mistrató, independientemente de su nivel jerárquico o su tipo de contratación. A su vez aplica, a los usuarios externos, proveedores y terceros que produzcan, administren, custodien o tengan acceso a la información del sistema de información de la Empresa.

## SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

Cuando se habla de seguridad informática, es primordial hacer la distinción en propósitos de protección, ya que se debe proteger la seguridad de la información, pero a su vez, es necesario proteger los datos. Es necesario destacar que, aunque se debe hacer una distinción entre los propósitos, generalmente las medidas de protección aplicadas serán las mismas.

En la seguridad de la información, el objetivo de la protección son los datos mismos y trata de evitar tanto su pérdida como su modificación no autorizada. Cuando hablamos de protección de datos, debemos garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos como por ejemplo la autenticidad. El móvil principal para implementar estas medidas de protección es el interés de la Empresa misma que maneja los datos, puesto que la pérdida de estos, puede generar un daño ya sea material o inmaterial; esto inherentemente puede generar pérdidas económicas u otras consecuencias negativas para la Empresa de Servicios Públicos de Mistrató.

En el caso de la protección de datos, el objetivo directo no es la protección de los datos en si mismo, sino el contenido de la información sobre las personas, para evitar el abuso de esta. Por tanto, el móvil para la protección de estos datos por parte de la Empresa es más una obligación jurídica orientada a la ética personal, con el fin de evitar consecuencias negativas para las personas de las cuales se trata la información.

## AMENAZAS

Una amenaza es una posibilidad de ocurrencia de cualquier tipo de evento o acción que pueda producir daño sobre los elementos de un sistema. En este caso particular es el riesgo de que dañen elementos de información. Desde la perspectiva de la Empresa, puede haber amenazas externas como por ejemplo hackers, daños físicos causados por personas o eventos naturales; a su vez puede haber amenazas internas como la negligencia del personal que maneja los equipos, falta de mantenimiento preventivo, entre otros. La gestión de estas amenazas debe estar concentrada en eliminar la probabilidad de ocurrencia, sin embargo, existen amenazas imposibles de eliminar, como son los virus de computadora. Para estos casos, se deben buscar medidas que mitiguen la probabilidad de ocurrencia del riesgo, para lo cual se pueden adquirir antivirus.

## DEBILIDADES

Las debilidades son las condiciones y características del sistema que lo hacen susceptible a amenazas, con el resultado de sufrir algún daño. Por lo tanto, el sistema debe estar en capacidad de responder a una amenaza o debería tener la facultad para recuperarse de un daño.

## GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El primer paso para la gestión de la seguridad y privacidad de la información, es la realización de un análisis de los riesgos, con el fin de determinar los componentes del sistema de información que requieran protección, detectar las debilidades que generen amenazas y lo pongan en peligro, con el fin de tomar determinaciones acerca de las medidas de prevención necesarias. Existen varios métodos para la valoración de un riesgo, los cuales se deben implementar de acuerdo a las políticas de administración del riesgo de la Empresa de Servicios Públicos de Mistrató.

Además del análisis de riesgo, es importante realizar una clasificación del flujo de información. Esta medida tiene como propósito el garantizar la protección de los datos personales por medio de la definición de diferentes niveles de autorización de acceso a los datos e informaciones. Teniendo en cuenta el contexto misional de la empresa, es necesario velar por la privacidad de la información privada con que se cuenta de los usuarios de los servicios públicos domiciliarios. La empresa ha definido cuales datos son de carácter público, cuales son de carácter privado.

En términos generales, todas las debilidades y amenazas que se puedan presentar en el sistema de información de la Empresa de Servicios Públicos, terminan derivando en la pérdida de información relevante o en su utilización con fines para los cuales no debería estar destinada, por esta razón, es primordial para la Empresa, la obtención y almacenamiento de copias de seguridad o Backups. Por este motivo, dentro de la Empresa se establece una directriz, indicando que semanalmente se deben realizar copias de seguridad en memorias USB de uso exclusivo para el almacenamiento de información importante de la Institución, con el fin de evitar traumatismos en el funcionamiento de la Empresa, donde se llegue a presentar una pérdida de información, ya sea por problemas de software o hardware.

**DIEGO ARMANDO BEDOYA MOSCOSO**
Gerente E.S.P. Mistrató