EMPRESAS PÚBLICAS MUNICIPALES DE SIBATÉ S.C.A. E.S.P

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN 1
2. DIRECCIONAMIENTO ESTRATÉGICO 2
   2.1. MISIÓN 2
   2.2. VISIÓN 2
   2.3. INTEGRIDAD 2
   2.4. POLÍTICA DE CALIDAD 2
   2.5. OBJETIVOS DE CALIDAD 3
3. NORMATIVIDAD 4
4. PLAN DE SEGURIDAD Y PRIVICIDAD DE LA INFORMACION 2023 5
   4.1. OBJETIVO GENERAL 6
   4.2. OBJETIVOS ESPECÍFICOS 6
   4.3. ALCANCE Y DELIMITACIÓN DEL PLAN 6
   4.4. HERRAMIENTAS PARA LA EJECUCIÓN DEL PROYECTO 6
   4.5. ACTIVIDADES PROHIBIDAS 8
   4.6. PRESUPUESTO 9
5. TERMINOS Y DEFINICIONES 10

1. INTRODUCCIÓN

Con el fin de garantizar el manejo eficaz de la información con la cual trabaja Empresas públicas municipales de Sibaté S.C.A. E.S.P. por medio de los equipos, aplicaciones informáticas y demás medios con los cuales interactúan diariamente los funcionarios y usuarios en general, se hace necesario identificar y gestionar las actividades que se relacionan con la Seguridad de la Información.

Esto se logra por medio de un Sistema de Gestión de Seguridad de la Información acorde con referentes nacionales e internacionales como la norma ISO 27001:2013, que permite la evaluación de riesgos, el establecimiento de controles, la evaluación de la conformidad de las partes interesadas, tanto internas como externas y contribuye en la ejecución de un plan de continuidad de negocio, de tratamiento de incidentes y de contingencia que son vitales para la institución, como medida preventiva ante cualquier eventualidad a la cual se pueda ver expuesta. Este Sistema de Gestión de Seguridad de la Información además permite el fortalecimiento de los procesos por medio del diseño, implementación y revaluación de la seguridad, lo cual arroja como resultado el mejoramiento continuo gracias a la adopción del modelo PHVA (Planear-Hacer-Verificar-Actuar).

Empresas Públicas Municipales de Sibaté S.C.A E.S.P
Teléfono: (57+1) 7250838 / PQR: Ext. 108
Dirección: Calle 4 N° 6 A - 77 Barrio San Jorge, Sibaté, Cundinamarca.
info@espsibate.com
www.espsibate.com
@espsibate
Nit. 900.171.710-9

2. DIRECCIONAMIENTO ESTRATÉGICO

2.1. MISIÓN

Proveer bienestar y salubridad a nuestros usuarios con la prestación servicios de acueducto, alcantarillado, aseo y complementarios de la mayor calidad, además proteger nuestro recurso hídrico y contribuir al desarrollo sostenible del Municipio de Sibaté.

2.2. VISIÓN

EPM - Sibaté en 2030 es reconocida por i). Proteger a nuestros usuarios, su bienestar y salubridad, prestando los mejores servicios de acueducto, alcantarillado, aseo y complementarios; ii). Proteger el agua; y iii). Contribuir al desarrollo sostenible del Municipio de Sibaté, especialmente por nuestros aportes a la cultura ciudadana y el medio ambiente.

2.3. INTEGRIDAD

- RESPETO
- HONESTIDAD
- COMPROMISO
- DILEGENCIA
- JUSTICIA

2.4. POLÍTICA DE CALIDAD

En Empresas Públicas municipales de Sibaté S.C.A. E.S.P. prestamos con transparencia los servicios de acueducto, alcantarillado, aseo y Servicios especiales y/o Complementarios, buscando la satisfacción de nuestros usuarios y clientes mediante el Mejoramiento continuo de nuestros procesos, procedimientos y prácticas. Apuntándole a Una mayor eficiencia, eficacia y efectividad en coherencia con el plan sectorial; con Compromiso de cumplimiento con la legislación colombiana aplicable y controlando los Riesgos que puedan entorpecer la operación. Todo esto apoyado en un equipo humano Comprometido y competente.

Empresas Públicas Municipales de Sibaté S.C.A E.S.P
Teléfono: (57+1) 7250838 / PQR: Ext. 108
Dirección: Calle 4 N° 6 A - 77 Barrio San Jorge, Sibaté, Cundinamarca.
info@espsibate.com
www.espsibate.com
@espsibate
Nit. 900.171.710-9

2.5. OBJETIVOS DE CALIDAD

- Garantizar la cobertura, dentro del área de prestación de los Servicios Públicos de Acueducto, Alcantarillado y Aseo en un 100%
- Garantizar en materia de calidad de agua, que las muestras no superen el 5% de IRCA
- Lograr como mínimo, un grado de satisfacción general del 90% en usuarios y clientes, con relación a los servicios prestados.
- Asegurar una comunicación eficaz con os usuarios y o clientes para los servicios de Acueducto, Alcantarillado, Aseo, Complementarios y Especiales.
- Incrementar ingresos por la prestación de los servicios públicos de Acueducto, Alcantarillado y Aseo en una taza del 5% anual.
- Incrementar ingresos derivados de otras operaciones diferentes a los servicios públicos.
- Contar con una planta de personal, con la educación y formación necesarias para el desempeño de sus funciones.
- Cumplir con el presupuesto previsto para la operación.
- Garantizar condiciones de trabajo seguras y saludables con el fin de evitar la ocurrencia de accidentes de trabajo y de enfermedades laborales.
- Implementar una gestión del riesgo, para asegurar el cumplimiento de los objetivos.

Empresas Públicas Municipales de Sibaté S.C.A E.S.P
Teléfono: (57+1) 7250838 / PQR: Ext. 108
Dirección: Calle 4 N° 6 A - 77 Barrio San Jorge, Sibaté, Cundinamarca.
info@espsibate.com
www.espsibate.com
@espsibate
Nit. 900.171.710-9

3. NORMATIVIDAD

El Sistema de Gestión de Seguridad de la Información de Empresas públicas municipales de Sibaté S.C.A. E.S.P. se ciñe a la normatividad legal vigente colombiana, tal como se describe enseguida:

- **Ley 527/99:** Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
- **Ley 594/00:** Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
- **Ley 850/03** establece en su artículo 9º: Principio de Transparencia.
- **Ley 1266/08:** Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- **Ley 1221 de 2008:** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **Ley 1273/09:** Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- **CONPES 3701 de 2011:** Lineamientos de política para ciberseguridad y Ciberdefensa.
- **Resolución 2886 de 2012:** Por la cual se definen las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo y se dictan otras disposiciones.
- **Ley 1581/12:** Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
- **Decreto 884 de 2012:** Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **Decreto 886 de 2014**: Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos.
- **Decreto Nacional 2573 de 2014:** Estrategia de Gobierno en Línea de la República de Colombia
- **LEY 1712 DE 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- **Decreto 103 de 2015**: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Empresas Públicas Municipales de Sibaté S.C.A E.S.P
Teléfono: (57+1) 7250838 / PQR: Ext. 108
Dirección: Calle 4 N° 6 A - 77 Barrio San Jorge, Sibaté, Cundinamarca.
info@espsibate.com
www.espsibate.com
@espsibate
Nit. 900.171.710-9

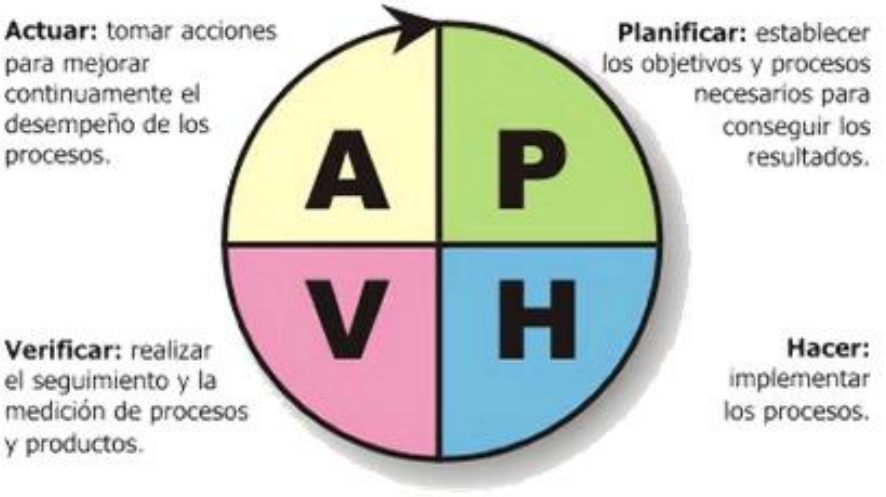
4. PLAN DE SEGURIDAD Y PRIVICIDAD DE LA INFORMACION 2024.

El Plan de seguridad y privacidad de la información es un documento de alto nivel que denota el compromiso de Empresas públicas municipales de Sibaté S.C.A. E.S.P. con la seguridad de la información. Este Plan contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la entidad apoyada en el uso adecuado de TICs.

Empresas públicas municipales de Sibaté S.C.A. E.S.P. debe salvaguardar las características de integridad, disponibilidad y confidencialidad de la seguridad de la información, mediante la adopción de políticas y procedimientos institucionales orientada al logro de sus objetivos estratégicos, en estricto cumplimiento de las normas vigentes. De este modo, la empresa velará por la adecuada gestión de los riesgos, la adopción de buenas prácticas en el uso de los activos de información y la mejora continua de las competencias del talento humano.

La eficiencia de la política de seguridad de la información se construye a través del liderazgo y compromiso de la Alta Dirección y la participación activa de los funcionarios, contratistas y terceros, quienes mancomunadamente deberán alcanzar el nivel de cumplimiento según los lineamientos y requisitos de seguridad de la información determinados aquí, así como el desarrollo de estrategias de mejora continua y gestión oportuna frente a incidentes o eventos de seguridad de la información.

El modelo a implementar es el ciclo PHVA, como metodología para la mejora continua.



Empresas Públicas Municipales de Sibaté S.C.A E.S.P
Teléfono: (57+1) 7250838 / PQR: Ext. 108
Dirección: Calle 4 N° 6 A - 77 Barrio San Jorge, Sibaté, Cundinamarca.
info@espsibate.com
www.espsibate.com
@espsibate
Nit. 900.171.710-9

4.1. OBJETIVO GENERAL

Planificar, orientar y desarrollar los mecanismos necesarios para dotar de disponibilidad, confidencialidad e integridad al conjunto de datos y activos de información de la Entidad.

4.2. OBJETIVOS ESPECÍFICOS

- Formular el esquema de seguridad de la información de acuerdo a las necesidades del Sistema de Información de Empresas públicas municipales de Sibaté S.C.A. E.S.P.
- Instaurar medidas de control de acceso a los activos de información de Empresas públicas municipales de Sibaté S.C.A. E.S.P.
- Alinear a la normatividad vigente las políticas de gestión y administración de activos de información
- Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información

4.3. ALCANCE Y DELIMITACIÓN DEL PLAN

El objetivo que se busca con la implementación de su SGSI es mejorar los niveles de seguridad de la información y la protección de los activos de información, para lograrlo sabe que es indispensable implementar los controles según lo señalado por el estándar ISO 27001:2013 y la normatividad vigente aplicable Por tal razón, los funcionarios, contratistas y terceros que interactúen con los activos de información de Empresas públicas municipales de Sibaté S.C.A. E.S.P. como ya se ha mencionado, deberán conocer y cumplir las políticas, procesos y procedimientos que hacen parte del SGSI, salvaguardando ante todo los principios de confidencialidad, integridad y disponibilidad que los protegen frente a cualquier tipo de tratamiento..

4.4. HERRAMIENTAS PARA LA EJECUCIÓN DEL PROYECTO

Finalmente, a continuación, se lleva a cabo una reseña de las principales características de la norma ISO/IEC 27001:2013, la cual se ha seleccionado como estándar para la implementación.

OBJETIVOS DE CONTROL:

- **Políticas de seguridad de la Información:** Establece la necesidad de definir un conjunto de políticas aplicadas a todas las actividades relacionadas con la gestión de la seguridad de la información dentro de la Organización, con el propósito de proteger la misma contra las amenazas presentes en el entorno.

- **Organización de la seguridad de la información:** Sugiere diseñar una estructura para la gestión de la seguridad de la información dentro la Organización que establezca los roles y responsabilidades con la seguridad de la información a lo largo de la misma.
- **Seguridad del Recurso Humano**: Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan. También determina cómo incide el papel que desempeñan los empleados como responsables de la seguridad de la información.
- **Gestión de Activos:** Detalla los elementos de la Organización (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad que permita garantizar un nivel adecuado de protección.
- **Control de acceso:** Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo, establece los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.) que requiere cada empleado de la Organización y el personal externo que brinda servicios, en concordancia con sus responsabilidades.
- Esto permitirá identificar y evitar acciones o actividades no autorizadas, garantizando los servicios informáticos.
- **Cifrado:** Garantiza el uso adecuado y eficaz del cifrado para proteger la confidencialidad, autenticidad y/o integridad de la información.
- **Seguridad física y ambiental:** Responde a la necesidad de proteger las áreas, los equipos y los controles generales. El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la Organización, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputo, PC de usuarios críticos, equipos de los proveedores de servicios, etc.), y áreas en las cuales se recibe o se almacena información (magnética o impresa) sensitiva (fax, áreas de envío y recepción de documentos, archivadores, etc.), minimizando riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.
- **Seguridad de las operaciones:** Define las políticas, procedimientos y responsabilidades para asegurar la correcta operación de las instalaciones de procesamiento de información.
- **Seguridad de las comunicaciones**: Define las políticas y procedimientos para asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Establece la necesidad de implantar medidas de seguridad y aplicación de controles de seguridad en todas las etapas del proceso de desarrollo y mantenimiento de los sistemas de información.

Además, considera los mecanismos de seguridad que deben implantarse en el proceso de adquisición de todos los sistemas o aplicaciones de la Organización, para prevenir pérdidas, modificaciones, o eliminación de los datos, asegurando así la confidencialidad e integridad de la información.

- **Relación con proveedores:** Permite asegurar la protección de los activos de información que son accedidos por proveedores.
- **Gestión de Incidentes de Seguridad:** Establece la necesidad de desarrollar una metodología eficiente para la generación, monitoreo y seguimiento de eventos e incidentes de seguridad.

4.5. ACTIVIDADES PROHIBIDAS

Pautas para tener en cuenta:

- Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.
- La distribución o instalación de software sin la licencia de uso adquirida
- Difundir información identificada como confidencial a través de medios que involucren el uso de la Tecnología de Información.
- Introducir software malicioso en la red o en los servidores (virus, envío masivo de correo electrónico, etc.)
- Utilizar la infraestructura de tecnología de información de Empresas públicas municipales de Sibaté SCA ESP para conseguir o transmitir material con ánimo de lucro. Igualmente se prohíbe el uso del sistema de comunicaciones de Empresas públicas municipales de Sibaté SCA ESP con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.
- Hacer ofrecimientos fraudulentos os de productos o servicios cuyo origen sean los recursos o servicios propios de Empresas públicas municipales de Sibaté SCA ESP
- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.
- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.
- Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El personal del área de Sistemas, es responsable de la Seguridad Informática y puede realizar estas actividades siempre y cuando sean previamente autorizadas por la dirección del departamento.
- Ejecutar cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada.

- Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
- Descargar archivos de gran tamaño que puedan afectar los canales de datos y comunicación de las compañías.
- Modificar la configuración de sistemas operativos, aplicativos de la Empresa, software antivirus, firewall personales o políticas de seguridad en general implantadas en los equipos de cómputo, sin consultar previamente con el área de Sistemas, la cual analizará la viabilidad de los cambios solicitados.

4.6. PRESUPUESTO

Las Empresas Públicas Municipales de Sibaté S.C.A. E.S.P, para la vigencia 2024, asigna el presupuesto de conformidad al Plan de adquisiciones aprobado.

Empresas Públicas Municipales de Sibaté S.C.A E.S.P
Teléfono: (57+1) 7250838 / PQR: Ext. 108
Dirección: Calle 4 N° 6 A - 77 Barrio San Jorge, Sibaté, Cundinamarca.
info@espsibate.com
www.espsibate.com
@espsibate
Nit. 900.171.710-9

5. TERMINOS Y DEFINICIONES

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

Amenaza: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Amenaza informática: la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).

Análisis de riesgos: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.

Autenticación: provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad: propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

Empresas Públicas Municipales de Sibaté S.C.A E.S.P
Teléfono: (57+1) 7250838 / PQR: Ext. 108
Dirección: Calle 4 N° 6 A - 77 Barrio San Jorge, Sibaté, Cundinamarca.
info@espsibate.com
www.espsibate.com
@espsibate
Nit. 900.171.710-9