PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AMABLE E.I.C.E.

ENERO DE 2023

INTRODUCCION

La Entidad ha reconocido la información como uno de los activos más importantes de la organización, haciendo necesaria la protección de la misma frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, de gestión pública, y de conformidad legal necesarios para alcanzar las metas con la formulación de la presente Política de Seguridad de la Información, AMABLE E.I.C.E , materializa la gestión responsable de información que proyecta garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos y metas trazadas en la administración pública.

CONCEPTOS BÁSICOS

La Seguridad Informática refiere las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Se evidencian tres conceptos fundamentales que representan las acciones durante el proceso, el primero la amenaza, la vulnerabilidad y finalmente la contramedida.

Considerar aspectos de seguridad significa:

- Conocer el peligro
- Clasificarlo
- Protegerse de los impactos o daños de la mejor manera posible.

Esto significa que solamente cuando se conoce las amenazas, agresores y sus intenciones dañinas (directas o indirectas) se pueden tomar medidas de protección adecuadas, para que no se vulneren los recursos valiosos.

“La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo”

La gestión del riesgo, partiendo desde la seguridad informática se divide en cuatro fases:

- Análisis: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- Reducción: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.

- Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

El proceso se basa en la política de seguridad, las cuales describen las normas y reglas institucionales, que forman el marco operativo en la entidad, logrando así:

- Fomentar las capacidades institucionales, reduciendo la vulnerabilidad y confinando las amenazas reduciendo así el riesgo.
- Guiar u orientar un funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Tomar medidas correctivas a las conductas o prácticas que hacen un sistema vulnerable.
- Sincronizar la coherencia entre las acciones pensar, decir y hacer.

La seguridad informática se enfatiza en propender a acceder a datos y recursos del sistema garantizando mecanismos de autentificación y control, para que los usuarios que accedan a estos recursos sólo posean los derechos que se les han configurado.

Estos sistemas de control de seguridad pueden causar inconvenientes a los usuarios. A medida del que la red crece las reglas de seguridad se vuelven cada vez más complicadas por lo que deben estudiarse monos que eviten que los usuarios desarrollen usos necesarios y así poder utilizar los sistemas de información de una forma segura.

Por esta razón, para asegurar la información se debe definir una política de seguridad que se pueda implementar en concordancia a las siguientes etapas:

- Conocer las necesidades de seguridad y los riesgos informáticos, así como sus posibles consecuencias.
- Tomar acciones preventivas que proporcionen las reglas y los procedimientos que se deben implementar para afrontar los riesgos identificados en los diferentes departamentos o secretarias de la organización.
- Detectar y controlar las vulnerabilidades del sistema de información, y mantener alerta para evitar posibles falencias en el control de las mismas.
- Desarrollar acciones correctivas que se puedan utilizar en caso de detectar una amenaza.

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- Confidencialidad: Los activos de información solo pueden ser accedidos y custodiados por usuarios que cuente con permisos para

ello.

- Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad
- Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que cuenten con los permisos adecuados.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad es un documento que denota el compromiso del Gerente de AMABLE E.I.C.E con la seguridad y privacidad de la información, la cual tiene como objetivo preservar, proteger y administrar de forma eficiente la información de AMABLE E.I.C.E junto con las medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

ALCANCE

Esta política de seguridad y privacidad de la información incluye terceros y a todo el personal de la Empresa independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

OBJETIVOS

- Preservar, proteger y administrar de forma eficiente la información de Empresa AMABLE E.I.C.E junto con las medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y controlada, enmarcada en el tratamiento de los riesgos de la información de AMABLE E.I.C.E, para asegurar la sostenibilidad de la misma y el nivel de eficacia.

RESPONSABILIDADES ASIGNADAS

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de AMABLE E.I.C.E, independiente del tipo de vinculación, el área o dependencia a la cual se encuentre adscrito y el nivel del cargo o funciones que desempeñe.

El comité institucional de gestión del desempeño es el responsable de formular, analizar y proyectar el documento de la política de seguridad y

privacidad de la información para que el Gerente lo avale. Es compromiso del Comité determinar las estrategias de capacitación de las políticas de seguridad y privacidad de la información en AMABLE E.I.C.E.

El coordinador del Comité deberá coordinar las gestiones para promover la socialización, seguimiento y control de la política.

Los propietarios de la información son los responsables de la producción, documentación, clasificación, actualización y valorización de la misma de acuerdo con los cargos desempeñados, funciones, competencias y acuerdos de confidencialidad a que haya lugar.

El Director Administrativo es el responsable de brindar la inducción al personal acerca de las obligaciones de seguridad y privacidad de la información.

En consecuencia AMABLE E.I.C.E se compromete a cumplir a cabalidad y de forma permanente con los preceptos que a continuación se mencionan.

a) Garantizar al titular de forma indefinida y permanente el pleno y efectivo respeto de sus derechos referidos a sus datos personales.

b) Conservar la información bajo estrictas medidas de seguridad con el fin de impedir pérdida, consulta uso o acceso no permitido o fraudulento.

c) Tramitar las consultas y reclamos interpuestos por los titulares de la información en los términos que para ello tiene fijado el artículo 14 de la Ley 1581 de 2012 en cuanto al tiempo de respuesta.

d) Permitir el acceso a la información únicamente a las personas que con ocasión de sus labores como empleados deban tener dicho acceso.

IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

La información cada área de AMABLE E.I.C.E debe actualizar el inventario de los activos de información a medida que se procese o produzcan unidades de datos.

SEGURIDAD DE LA INFORMACIÓN EN EL TALENTO HUMANO

Cada funcionario y contratista de AMABLE E.I.C.E, independiente del tipo de vinculación laboral debe contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado.

El área de sistemas debe mantener actualizado un directorio completo y actualizado de los perfiles creados.

Desde la Dirección Administrativa se determina cuáles son los privilegios que tendrían los diferentes perfiles del personal, a su vez debe elaborar, mantener, actualizar, mejorar y difundir las responsabilidades Personales para la seguridad de la información de la Entidad. La responsabilidad de la preservación de documentos y cuidado de la información de personal que se retira o cambia de cargo, la asume el respectivo supervisor del contratista.

ASUNTOS OPERACIONALES Y DE MANEJO

Para que la Política de seguridad y privacidad de la información sea práctica, AMABLE E.I.C.E debe utilizar las mejores prácticas y procedimientos para cumplir con las estrategias de preservación y cuidado de la información como la documentación de la generación y el control de cambios de las unidades de datos, estos deben ser establecidos e implementados en la Entidad para proveer una protección adecuada de los activos de la información.

RESPONSABILIDADES DEL PERSONAL

Los servidores públicos y contratistas de AMABLE E.I.C.E deben suscribir un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de Tecnologías de la información y las reglas que autorizan el uso de la información generada en la Entidad. El Director Administrativo y el contratista de apoyo en sistemas de la entidad se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que proyecte la socialización y concientización individual y colectiva en temas de seguridad de la información en todo el personal.
El contratista de apoyo de la Entidad es el responsable de realizar los procedimientos para crear los respectivos perfiles y los privilegios de cada funcionario o contratista de acuerdo a los lineamentos en cuanto al uso de los dispositivos de hardware y los elementos de software, además, deberá publicar en medios impresos y virtuales como intranet, correo electrónico, entre otros, información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de documentos, archivos, buenas prácticas, amenazas de seguridad, entre otros.

RESPONSABILIDADES DE USUARIOS EXTERNOS

El personal de empresas externas deben estar autorizados por una persona designada por parte de AMABLE E.I.C.E para controlar y supervisar el uso adecuado de la información y procurar por la buena utilización de recursos tecnológicos.

Los procedimientos para el uso adecuado de los recursos tecnológicos y de la información deben ser diseñados e implementado por el contratista de sistemas. Los dueños de los activos de la información se encargaran de

orientar a los usuarios externos autorizados para que hagan adecuado uso de la información y componentes tecnológicos facilitados.

Todos los usuarios externos sin excepción deben aceptar por escrito los términos y condiciones de uso de la información y recursos Tics institucionales.

ADMINISTRACION DE LAS COMUNICACIONES Y OPERACIONES REPORTE Y REVISIÓN DE INCIDENTES DE SEGURIDAD

El contratista de sistemas de AMABLE E.I.C.E notificará al Gerente y a la Dirección Administrativa de la Entidad las novedades que se presenten a nivel de seguridad, claramente cuando amerite y se presenten situaciones específicas el mismo funcionario afectado realizará el reporte respectivo; describirá la solicitud y las actividades de solución.

Entre tanto, el contratista de sistemas realizará procedimientos específicos para la actualización de las bases de antivirus, el análisis y búsqueda de amenazas en los equipos de cómputo sin que esto suponga un impacto alto o una prolongada interrupción en el desarrollo normar de actividades de la Entidad.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING.

A nivel administrativo, físico y técnico se deben proteger todos los sistemas de información como control básico, todas las estaciones de trabajo de AMABLE E.I.C.E deben estar protegidas por software antivirus, cabe recordar que los usuarios de cada puesto de trabajo no están autorizados para deshabilitar las opciones de protección del antivirus en sus diferentes enfoques, tales como, antivirus para archivos, antivirus para la web, supervisor de software malicioso y buscador de objetos peligrosos.

COPIAS DE SEGURIDAD

Toda información que sea valorada como activo de información corporativa debe ser respaldada con copias de seguridad (backups) con la periodicidad que determine el encargado del área de sistemas de la Entidad y almacenada en el disco externo en carpetas por área según corresponda. El área de sistemas debe proveer la herramienta para que los funcionarios y contratistas puedan consultar el registro de la información y las copias de seguridad.

ADMINISTRACIÓN DE REDES DE ÁREA LOCAL.

La configuración de terminales de red, enrutadores, switches, firewall y los

sistemas de seguridad de red a que haya lugar; debe ser documentada, resguardada como copia de seguridad y mantenida por el contratista de sistemas de la Entidad.

INTERCAMBIO DE INFORMACIÓN CON ENTIDADES EXTERNAS

Las solicitudes de información por parte de entes externos a AMABLE E.I.C.E deben ser primero aprobadas por la Directora de Control interno y en calidad de enlace posteriormente solicitado a los responsables del manejo custodia de dichos activos de información.
Estas peticiones de información deben ser realizadas por un medio válido que permita el registro de la solicitud, donde pueda identificarse el remitente, el asunto y la fecha toda la información de la Entidad debe ser manejada de acuerdo a la legislación colombiana y según la normatividad vigente.

INSTALACIÓN DE SOFTWARE

Todas las instalaciones de software que se realicen sobre los sistemas operativos previamente instalados en AMABLE E.I.C.E, deben ser autorizados por el Gerente y/o por el Director Administrativo bajo la supervisión del contratista de Sistemas.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. El contratista de Sistemas debe desinstalar cualquier software ilegal, al igual debe mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

CONTROL DE CLAVES Y NOMBRES DE USUARIO

Cada funcionario o Contratista se debe autenticar para iniciar sesión en su equipo de cómputo con una contraseña previamente asignada para garantizar que cada uno sea el responsable de la transformación y custodia de la información institucional allí generada, igualmente, las cuentas de usuario para acceder a los sistemas de información con que cuenta la Entidad deben ser únicas y creadas para la persona que tiene esas funciones designadas, ese rol tendrá ciertos privilegios dentro de cada software según corresponda.

SEGUIMIENTO

El contratista de Sistemas hará seguimiento sobre el Uso que se haga de los recursos de tecnologías de la información en AMABLE E.I.C.E por parte de algún funcionario autorizado, en caso de encontrarse alguna novedad lo reportará ante el Gerente y Director Administrativo.

CUMPLIMIENTO

Toda compra de hardware y adquisición y/o desarrollo de software en AMABLE E.I.C.E y todo uso y seguimiento de los recursos de Tecnologías de la información y las comunicaciones en la Entidad, debe estar sujeta a normas y estatutos internos así a la legislación nacional.

POLÍTICAS DE PRIVACIDAD Y CONDICIONES DE USO

Se considera norma de confidencialidad y protección de datos toda aquella información personal que el usuario ingresa libre y voluntariamente al Portal Web de AMABLE E.I.C.E www.armeniaamable.gov.co, la entidad no se hace responsable por los daños y/o perjuicios ocasionados por el uso inapropiado de la información o datos derivados de la página web en aras del incumplimiento de la política de seguridad de la información y protección de datos personales.

El portal web de la entidad, adopta una política de confidencialidad y protección de datos, con el objetivo de salvaguardar la privacidad de la información personal de sus usuarios obtenida a través de su sitio Web y se reserva el derecho de modificar o actualizar las Normas de confidencialidad y Protección de Datos que se describen más adelante con el fin de adaptarse a nuevos requerimientos legislativos o técnicos que permitan brindar mejores servicios y contenidos informativos, por lo cual se sugiere consultar estas normas periódicamente.

La entidad desde su portal web www.armeniaamable.gov.co actúa de buena fe al publicar documentos elaborados con fuentes propias y procura garantizar la disponibilidad, veracidad y confidencialidad de los mismos. No obstante, no se hace responsable de la precisión y actualización de la información suministrada por entidades externas que sean difundidos en el sitio web La Entidad, se reserva el derecho a introducir modificaciones o interrumpir los servicios ofrecidos, sin previo aviso a sus usuarios.

ABG. JAMES CASTAÑO HERRERA
Gerente

Elaboró: Johan Mauricio Castañeda Morales- Área de Planeación
Aprobó: Gerente – James Castaño Herrera – Comité institucional