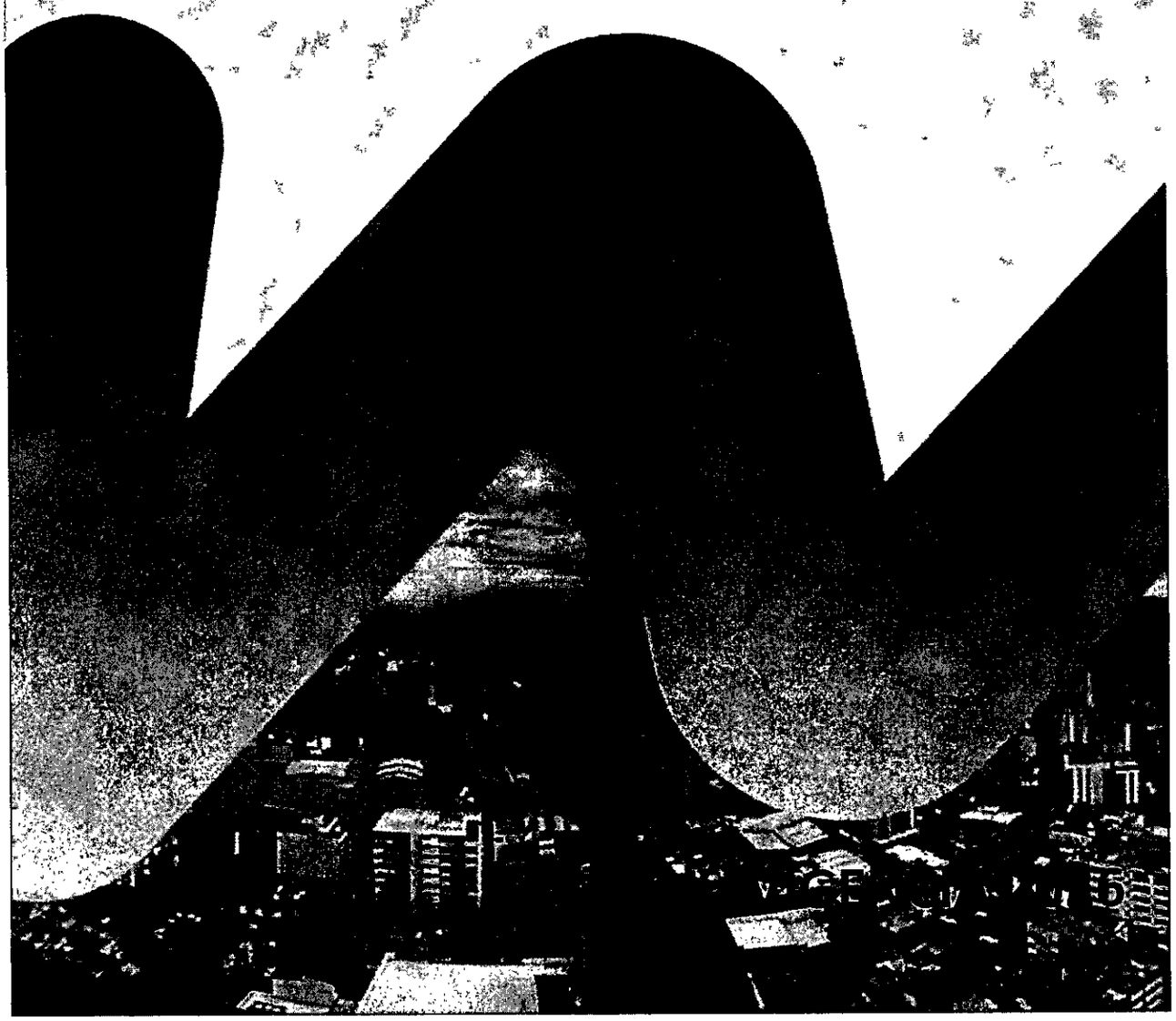
SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO AMABLE E.I.C.E.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



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,

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 e identificar 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 de la entidad.

"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 vulnerabilidady 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 unsistema 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.

PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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

- **Autenticidad**: Principio que garantiza veracidad en la autoría de la información. sin embargo, no garantiza la veracidad del contenido de la información. La autenticidad garantiza la veracidad del autor, de quien la produjo la información, sin importar si el contenido es verdadero o falso.

- **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

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 EmpresaAMABLE E.I.C.E junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las 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 yel nivel de eficacia.

CONCEPTOS Y DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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

- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias

grado en el que se cumplen los criterios de auditoría.

• **Autorización:** Consèntimiento previo, expreso e informado del Titular para el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

• **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

• **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

• **Ciberespacio:** Es el ambiente físico y virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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

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

• **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

• **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

• **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

• **Datos Personales Privados:** Dato que por su naturaleza intima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3, literal h).

• **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

• **Derecho a la Intimidad:** Derecho fundamental cúyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultura (Jurisprudencia Corte Constitucional).

• **Encargado del Tratamiento do Datos:** Persona natural o jurídica, pública o privada, que por si misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

• **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

•**Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

• **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 8).

• **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1286 de 2008.

• **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

• las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

• **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

• **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

• **Responsabilidad Demostrada:** Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

• **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos.

• **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/EC 27000).

• **Seguridad de la Información:** Preservación de la confidencialidad, Integridad, y disponibilidad de la información en cualquier medio: impreso o digital.

• **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la Información que se encuentra en medios digitales.

• **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

• **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

• **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

• **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

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.

Amable E.I.C.E, mediante la adopci6n e implementación de esta política pretende proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de sus activos de información .

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 yde 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.

e) Gestionar los riesgos de los activos de información teniendo en cuenta el nivel de tolerancia al riesgo de la empresa.

f) Realizar la gesti6n integral de los riesgos basados en la implementación de controles físicos y digitales orientados a la prevención de incidentes.

g) implementar las políticas de seguridad de alto nivel y complementarias por cada dominio de la norma Iso/IEC 27001 de 2013 para asegurar la confidencialidad, integridad y disponibilidad de la información institucional.

h) Fomentar la importancia de la seguridad de la información con los funcionarios, contratistas, proveedores y terceros.

i) Se deberán mitigar los incidentes de Seguridad y Privacidad de la información, Seguridad Digital de forma efectiva, eficaz y eficiente, y se protegerá la informaci6n creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un usa incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la informaci6n de su propiedad o en custodia.

DEBERES INDIVIDUALES DEL PERSONAL ADSCRITO A LA EMPRESA

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 encargaran 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 otro

Los usuarios de la información de la Empresa Amable E.I.C.E deberán cumplir con los siguientes deberes:

a) Usar la información de la Empresa Amable E.I.C.E únicamente para propósitos del negocio autorizado y en cumplimiento de su labor.

b) Respetar la confidencialidad de la información de la empresa Amable E.I.C.E.

c) No compartir perfiles de usuario, contraseñas, sesiones en estaciones de trabajo, documentos o cualquier tipo de información confidencial.

d) No anotar y/o almacenar en lugares visibles las contraseñas de acceso a los sistemas.

e) Ajustarse a las directrices de clasificación de la información.

f) Bloquear la sesión de la estación de trabajo al momento de ausentarse de la misma.

g) Las impresiones deben ser recogidas al momento de generarlas, no se deben dejar por largos periodos de tiempo en la impresora.

h) Devolver y no conservar ningún tipo de copia de sus activos de información en buen estado, una vez cese su relación laboral o contractual con la empresa.

i) Esta estrictamente prohibido la divulgación, cambio, retiro o perdida no autorizada de información de la entidad almacenada en medios físicos removibles, como USB, cintas magnéticas, discos duros entre otros.

j) Esta estrictamente prohibido utilizar software no licenciado en los recursos tecnológicos. Copiar software licenciado de la Empresa Amable E.I.C.E, para utilizar en computadores personales, ya sea en su domicilio o en cualquier

otra instalación y/o entregarlos a terceros.

DEBERES DE LOS RESPONSABLES DEL PERSONAL ADSCRITO A LA EMPRESA

a) Conceder autorizaciones de acceso a la información acorde con las funciones a ser realizadas los funcionarios o contratistas.

b) Asegurar que los privilegios de acceso individuales reflejen una adecuada segregación de funciones. Un usuario no debe tener los permisos suficientes para originar, registrar y corregir/verificar una transacción sensitiva del negocio sin controles adecuados o una revisión independiente.

c) Restringir el acceso del personal a aquellas áreas que hayan sido restringidas por razones de seguridad.

d) Ser el responsable de conocer, solicitar y ratificar los privilegios de acceso a los empleados que le reportan.

e) Conservar los registros de los empleados con privilegios de acceso a la información. Adicionalmente, el profesional encargado del área TIC o Sistemas de la empresa como encargado de la Seguridad de la información, debe mantener actualizadas las autorizaciones y perfiles de usuario basándose en los archivos de Recursos Humanos y/o, donde se encuentran todos los empleados y las áreas a las que pertenece.

f) Los contratos de Outsourcing o con terceras personas, deben identificar claramente los acuerdos relacionados con la propiedad de la información y la no divulgación de información confidencial.

RESPONSABILIDADES DE USUARIOS EXTERNOS

El personal de las empresas externas debe estar autorizado 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 encargarán 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.

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.

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.

Inventario de activos

A través del equipo o comité institucional se identificará los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación. El Responsable de cada Unidad Organizativa involucrada deberá elaborar un inventario con dicha información y deberá actualizarlo ante cualquier modificación de la información registrada y revisarlo con una periodicidad semestral.

Clasificación de la información

Para clasificar un Activo de información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

a) Confidencialidad

Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea funcionario, contratista o no. PUBLICO

información que puede ser conocida y utilizada por un grupo de funcionarios o contratistas de la entidad, que la necesiten para realizar su trabajo, y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o perdidas leves a la empresa Amable E.I.C.E o terceros. CLASIFICADA -USO INTERNO

información que solo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la empresa Amable EICE o a terceros. CLASIFICADA - CONFIDENCIAL

información que solo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la empresa Amable E.I.C.E, y cuya divulgación o usos no autorizados podría ocasionar perdidas graves a la empresa o a terceros. CLASIFICADA -SECRETA

b) Integridad:

- información cuya modificación no autorizada, si no es detectada, no afecta la operatoria de la empresa.
- información cuya modificación no autorizada, si no es detectada, podría ocasionar perdidas leves para la empresa o terceros.
- información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas significativas para la empresa o terceros.
- información cuya modificación no autorizada, si no es detectada, podría ocasionar perdidas graves a la empresa o a terceros.

Clasificación y control de activos

Disponibilidad: Se distinguen dos casos:

inaccesibilidad transitoria:

- información cuya inaccesibilidad transitoria no afecta la operatoria de la empresa.
- Información cuya inaccesibilidad transitoria durante 1 semana podría ocasionar pérdidas significativas para la empresa o terceros.
- Información cuya inaccesibilidad transitoria durante 1 día podría ocasionar pérdidas significativas a la empresa o a terceros.
- Información cuya inaccesibilidad transitoria durante 1 hora podría ocasionar pérdidas significativas a la empresa o a terceros.

inaccesibilidad permanente:

- información cuya inaccesibilidad permanente no afecta la operatoria de la empresa.
- Información cuya inaccesibilidad permanente podría ocasionar perdidas leves para la empresa o terceros.
- Información cuya inaccesibilidad permanente podría ocasionar perdidas significativas para la empresa o terceros.
- información cuya inaccesibilidad permanente podría ocasionar perdidas graves a la empresa o a terceros.

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 quetendrían 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.

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.

a) Términos y condiciones para clientes de Internet:

La empresa Amable E.I.C.E asume que todos los clientes que usan Internet para establecer relación con la empresa aceptan los términos y condiciones impuestos por la misma en sus términos y condiciones de uso del portal de internet, antes de realizarse cualquier transacción.

b) Acuerdos con terceros que manejan información o cualquier recurso informático de la empresa:

Todos los acuerdos relacionados con el manejo de información o de recursos de informática de la empresa por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta clausula debe permitirle a la empresa ejercer auditoria sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información.

c) Definición clara de las responsabilidades de seguridad informática de terceros:

Proveedores, usuarios y otros asociados a los negocios de la empresa Amable E.I.C.E deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos.

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 comola 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

amenazas de seguridad, entre otros.

ADMINISTRACION DE LAS COMUNICACIONES Y OPERACIONESREPORTE 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.

Los computadores personales deben mantener activo un software antivirus, sistemas operativos, Microsoft Office, licenciados y actualizados y que su uso haya sido autorizado por el profesional o área T[C o de Sistemas de la empresa.

Cualquier información que venga por medio electrónico o de almacenamiento, como correo electrónico o información de internet, debe ser revisada por un software antivirus antes de ser descargada y utilizada.

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.

a) Periodo de almacenamiento de registros de auditoria:

Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un periodo no menor a tres (3) meses. Durante este periodo los registros deben ser asegurados para evitar modificaciones y para que puedan

registros son importantes para la correcci6n de errores, auditoria forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.

b) Tipo de datos a los que se les debe hacer backup y con qué frecuencia:

A toda información sensible y software critico de la empresa residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por el procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

c) Copias de información sensible:

Se debe elaborar una copia de cada backup con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco, según procedimiento de copias de respaldo.

USO DEL FIREWALL

a) Deteccion de intrusos:
Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

b) Toda conexión externa debe estar protegida por el firewall:
Toda conexión a los servidores de la empresa proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la empresa.

c) Toda conexión hacia Internet debe pasar por el Firewall:
El firewall debe ser el único elemento conectado directamente a Internet o servicio de internet, por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

d) Filtrado de contenido activo en el Proxy:
El encargado TIC o de sistemas de la empresa, debe asegurar que, dentro de las definiciones de políticas, se filtre todo contenido activo como applets de java, adobe flash player, controles de Activex debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información de la empresa.

e) Firewall debe correr sobre un computador dedicado o appliance:
Todo firewall debe correr sobre un computador dedicado o modelo appliance para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

f) inventario de conexiones:
Se debe mantener un registro de las conexiones a redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización, lo

anterior se cumple con el diagrama de red.

g) El sistema interno de direccionamiento de red no debe ser público:
Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

g) Revisión periódica y reautorización de privilegios de usuarios.
Los privilegios otorgados a un usuario deben ser reevaluados periódicamente con el fin de analizar si los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales.

Esta política debe ser ejecutada por el área de sistemas con la participación de cada uno de los coordinadores de área, quienes harán la revisión y solicitud de cambios a la gerencia.

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.

Existe una política de acceso por MAC ADDRESS registrada, lo cual no permite conectar equipos tales como switch, routers, access point, portatiles, tablets, celulares o cualquier otro dispositivo a la red de Amable E.I.C.E sin previa autorización de la Gerencia del administrador de la misma.

El equipo que requiera estar conectado a la red de datos debe ser registrado con anterioridad para que pueda ser conectado.

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 software autorizado para su uso e instalación en los sistemas informáticos institucionales.

La instalacion de software que se realicen sobre los sistemas operativos estará bajo la responsabilidad del profesional TIC o de Sistemas, realizando la coordinación y ejecución de mantenimiento de programas o aplicaciones instaladas en las estaciones o equipos de trabajo

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 paragarantizar que cada uno sea

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.

Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que debe cumplir con algunas de las siguientes características:

Incluir combinaci6n de números, letras mayúsculas, minúsculas y caracteres especiales.

A continuación, se especifican los controles requeridos para las contraseñas:

- Los perfiles de usuario y la contraseña tienen que ser asignados individualmente para soportar el principio de responsabilidad individual.
- Los usuarios no pueden prestar su contraseña, lo que se realice con su perfil queda bajo la responsabilidad del dueño.
- El usuario no debe compartir, escribir o revelar su contraseña.
- Las contraseñas individuales no deben ser mostradas en texto claro. Todos los sistemas de procesamiento deben eliminar la visualización de contraseñas ya sea en pantallas o en impresoras.
- Las contraseñas deben cambiarse con regularidad. La duración máxima de la contraseña debe ser un tiempo razonable (máximo 60 días).
- Si un sistema no obliga al cambio de contraseña, es responsabilidad del usuario realizar este cambio.
- No se deben repetir contraseñas utilizadas anteriormente, en los últimos cinco cambios.
- Debe verificarse la identidad del usuario antes de que las contraseñas o perfiles de usuario sean habilitados nuevamente. Solo se puede cambiar una contraseña cuando el perfil de usuario pertenezca a quien solicita el cambio.
- La identificación del usuario y su contraseña no deben ser iguales.

Las contraseñas deben ser cuidadosamente seleccionadas para que no sean adivinadas fácilmente, por lo tanto, se deben tener en cuenta las siguientes recomendaciones:

a) No utilizar el primer o segundo nombre, los apellidos, el nombre del esposo, el nombre de sus hijos, etc., en ninguna forma (reversado, diminutivos, etc.)

b) No utilizar otra información fácil de obtener acerca de Usted.
Esto incluye:

marca, nombre del edificio, etc.

c) No use contraseñas que contengan solo números o solo letras.

d) No utilice palabras contenidas en el diccionario u otras listas de palabras.

j) Use contraseñas fáciles de recordar para que no tenga que escribirlas.

f) No use el nombre del perfil de usuario en ninguna forma como, por ejemplo: reversado o duplicado.

Siempre que el Administrador de contraseñas asigne una contraseña, es responsabilidad del usuario cambiarla en su primer uso.

UTILIZACION DEL CORREO ELECTRONICO, ACCESO A INTERNET E INTRANET

Esta política pretende garantizar el uso efectivo del tiempo laboral, evitando el uso inapropiado del correo electrónico, internet e intranet.

El correo electr6nico es proporcionado al personal con el objetivo de ayudarle a llevar a cabo sus funciones de manera eficiente y eficaz, permitiendo la comunicación con los demás miembros del personal, otras empresas y entidades asociadas. El acceso a Internet en Amable E.I.C.E está controlado por las políticas internas de la seguridad de la información.

Los servicios de correo electrónico, internet e intranet de la empresa Amable E.I.C.E son para uso laboral; no debe ser utilizado para temas personales.

Uso del correo electrónico:

a) Cuando se utilizan los medios electr6nicos de la empresa Amable E.I.C.E para el acceso al correo electrónico, debe cumplirse con las siguientes pautas:
   - Consultar su correo electrónico diariamente.
   - Incluir una línea de asunto significativo en su mensaje.
   - Comprobar la línea de direcci6n antes de enviar un mensaje y verificar que lo envié a la persona adecuada.
   - Respetar las protecciones legales a los datos y software proporcionados por derechos de autor y licencias.

b) La herramienta de correo electrónico utiliza un filtro corporativo para evitar que se reciba contenido malicioso.

c) Todos los mensajes de correo electrónico emitidos por usuarios de la empresa Amable E.I.C.E que sean dirigidos a direcciones de correo externas, que contengan información confidencial, deben incluir una nota (Responsabilidad) como la que se muestra a continuación:

"Este mensaje, incluyendo cualquier archivo adjunto, puede contener

y/o de propiedad exclusiva y está destinado exclusivamente a la persona o personas a las que va dirigido. Si no es el destinatario previsto o ha recibido este mensaje por error, notifíqueselo de inmediato al remitente respondiendo a este correo electrónico y elimine permanentemente el original enviado por el remitente, incluidos los archivos adjuntos si los hay, sin hacer copias de los mismos."

POLITICA DE ESCRITORIO LIMPIO

El término "escritorio limpio" se refiere a la práctica de mantener ordenados y seguros los espacios de trabajo físicos y digitales. Para esto se deberán implementar acciones y directrices que conlleven a la materializaci6n y ejecución de las mismas, tales como:

Documentación y Sensibilización:

- Proporcionar a los empleados y contratistas la documentación clara sobre la importancia de mantener escritorios limpios para la seguridad informática.
- Realizar sesiones de sensibilización para destacar los riesgos asociados con la desorganización y la exposición de información sensible.
- instruir al personal de la empresa tanto empleados como contratistas para que eliminen de manera segura y periódica documentos impresos que contengan información confidencial.
- Proveer contenedores seguros para la destrucción de documentos.

Bloqueo de Pantalla:

- implementar la política de bloquear automáticamente las pantallas después
  de un periodo breve de inactividad.

- Exigir contraseñas seguras o autenticación biométrica para desbloquear las
  pantallas.

Recepción de Visitantes:

- Establecer procedimientos para garantizar que los visitantes no tengan acceso no autorizado a escritorios y pantallas.

- Proporcionar áreas seguras para que los visitantes esperen.

Almacenamiento Seguro de Documentos:

- Instruir a los empleados y contratistas a almacenar documentos sensibles de manera segura, como en cajones cerrados o armarios con llave.
- Evitar dejar documentos importantes en escritorios durante periodos prolongados.

Protección de Dispositivos de Almacenamiento:

- Prohibir el uso de dispositivos de almacenamiento externos no autorizados
  o no cifrados.
- Establecer políticas claras sobre la conexi6n y el uso de unidades USB y otros dispositivos similares.

Política de Escritorios Digitales:

- Implementar políticas de escritorios digitales limpios, lo que implica cerrar sesión en sistemas y aplicaciones cuando no se están utilizando.
- Prohibir compartir contraseñas y exigir el cierre de sesión al abandonar un escritorio.

Limpieza Física:

- Programar rutinas de limpieza física en las áreas de trabajo para reducir la
  acumulación de polvo y la posibilidad de que documentos importantes queden expuestos.

Gestión de Cables:

- implementar políticas para gestionar los cables de manera ordenada, reduciendo el riesgo de tropiezos y manteniendo un ambiente más ordenado.

INCIDENTES DE SEGURIDAD

Evaluar el tipo de vulnerabilidad detectado e identificar el tipo de incidente, sobre los siguientes tipos de ataques posibles:

- Spoofing: este tipo ataque consiste en suplantar o fa[sjficar un portal. Para esto es necesario monitorear los servidores de gestor de contenjdos (ej: joomla, wordpress, etc). Una vez se identifique si hubo una vulnerabilidad se eliminan los archivos que crean el spoofing y se restringen los permisos
  en la carpeta donde se ubicaron dichos archivos.

- Dos : Este ataque se define como Denial of Service y consiste en saturar los procesos de un portal y/o servidor mediante peticiones, las cuales provocan que se incrementen el consumo de recursos de los servidores causando así que se saturen y evitando la caída de mismo. Esto se detecta mediante el monitoreo de los recursos del servidor. Si se observa un consumo de recursos pico, se identifica de donde provienen las peticiones.
  Una vez identificado su origen, se bloquea dicho origen a través del firewall mediante bloqueo de Ip. Adicional a esto se implementa una herramienta que detecta bajo un parámetro establecido, cuantas peticiones debe recibir un servidor de forma regular. En caso de que este parámetro o umbral se supere, la herramienta rechaza todas las

de seguridad.

Una vez evaluado el ataque e implementada una solución, se procede a efectuar procedimientos de mayor envergadura para que no se repitan dichos ataques.

Como medidas preventivas, en el firewall se implementan políticas de seguridad más agresivas. Se realiza restricción de puerto en general dejando como excepción los puertos por el cual los servicios están publicados. Se eliminan o se restringen accesos a los servidores mediante cambio de contraseñas de manera más frecuente y se eliminan permisos de escritura sobre determinadas carpetas del servidor.

PRUEBAS DE RESTAURACION

La realización de pruebas de restauracion es una parte crucial en la política de seguridad informática para garantizar la integridad y el correcto funcionamiento de las bases de datos y los sistemas de la empresa.

Para esto se presenta el proceso general que se deberá seguir para llevar a cabo pruebas de restauración de bases de datos:

Planificación y Documentación:

- Definir un plan detallado que incluya los procedimientos específicos para llevar a cabo las pruebas de restauración.
- Documentar la información esencial, como la ubicación de los archivos de respaldo, las versiones de software utilizadas, y cualquier parámetro relevante.

Creación de un Entorno de Pruebas:

- Configurar un entorno de pruebas que sea lo más similar posible al entorno de producción.
- instalar el software de base de datos y otros componentes necesarios en el entorno de pruebas.

Restauración de Respaldo:

- Utilizar copias de seguridad recientes y válidas para llevar a cabo la restauración en el entorno de pruebas.
- Seguir los procedimientos definidos en el plan para restaurar las bases de datos.

Verificación de integridad:

- Verificar la integridad de los datos restaurados. Puedes utilizar herramientas de verificación de integridad proporcionadas par el sistema de gestion de bases de datos (DBMS).
- Comprobar que los datos restaurados coincidan con las expectativas y que no haya corrupción.

Pruebas de Funcionalidad:

- Realizar pruebas para asegurarse de que todas las funciones críticas del sistema y de la base de datos están operativas.
- Verificar la conectividad, la disponibilidad y el rendimiento de la base de datos restaurada.

Registro de Resultados:

- Documentar los resultados de las pruebas, incluyendo cualquier problema encontrado y las acciones correctivas tomadas.
- Asegurar mantener un registro detallado para futuras referencias y auditorias.

Mejoras Continuas:

- Evaluar regularmente y actualizar el plan de pruebas de restauración para Incluir nuevos escenarios o cambios en la infraestructura.
- Aprender de las pruebas anteriores para mejorar los procesos y la eficacia de las restauraciones.

Capacitación del Personal:

- Asegurarse de que el personal encargado de llevar a cabo las pruebas este
  debidamente capacitado y conozca los procedimientos a seguir.

Programación Regular:

- Programar pruebas de restauración de manera regular, no solo como un evento técnico. Esto garantizara que el proceso este siempre actualizado y
  que el personal este preparado.

Al seguir este proceso, se podrá verificar la capacidad de Amable E.I.C.E para recuperarse de posibles pérdidas de datos y asegurar la integridad de las bases de datos en situaciones de emergencia.

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.
De igual manera se realizará la revisión a la presente política de seguridad y los objetivos planteados.

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 dela información y las

comunicaciones en la Entidad, debe estar sujeta anormas y estatutos internos así a la

legislación nacional.

Esta política interna de seguridad y privacidad de la información deberá revisarse y actualizarse cada año o cuando se considere pertinente por cambios normativos o necesidades del servicio, riesgos de seguridad que así lo ameriten.

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.

JAMES CASTAÑO HERRERO
Gerente

Elaboró: Leonardo Sánchez Ariza - Contratista
Revisó: Gabriela Giraldo Contratista Profesional Líder Administrativa y Financiera.
Aprobó: Gerente – James Castaño Herrera – Comité Institucional