PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VIGENCIA 2020

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

INTRODUCCIÓN

El Plan de Gestión de Seguridad de la Información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, por una parte, los elementos fundamentales para preservar la confidencialidad, integridad y disponibilidad de la información, y por otra, determina los métodos, procedimientos y vigilancias que se deben aplicar conforme a la legislación colombiana y a las necesidades y objetivos estratégicos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

Para obtener este objetivo, las estrategias definidas que brindan los instrumentos necesarios para que los funcionarios, contratistas y terceros que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI en adelante) de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES obtengan preservar los controles pretendidos para asegurar la información.

En la presente y variable colectividad de la información, toda entidad pública o privada debe lograr una adecuada articulación entre el SGSI y las políticas de seguridad de la información, esto se consigue a través de la composición de políticas, ordenamientos, sistemas de información y controles con el objetivo de gestionar de manera oportuna e ipso facto los riesgos, de tal forma que las partes interesadas obtengan un alto desempeño de seguridad y confidencia.

Se deduce, que las políticas deben ser plenamente distinguidas y ejecutadas por los funcionarios, contratistas y terceras partes que tienen acceso a los activos de información y a los sistemas de procesamiento de información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES para una optimización de los procesos en cuanto a seguridad informática, es preciso que sus esfuerzos y capacidades se agrupen en lograr los fines fundamentales de las políticas, como organizar controles para salvaguardar los activos de información; incentivar conciencia en los usuarios acerca del uso responsable de las tecnologías de la información y comunicaciones.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La información es un recurso que, como el resto de los activos, tiene valor para la entidad y por consiguiente debe ser debidamente protegida. El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto del Sistema de información.

En la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la administración de riesgos y la consolidación de una cultura de seguridad.

La información, en sus múltiples códigos y formas, así como los trámites y servicios que las entidades del Estado proveen a los ciudadanos se consideran un bien público. En ese sentido, los activos de información que conforman los bienes y servicios que proveen las entidades públicas son activos públicos y por lo tanto, deben protegerse adecuadamente.

Consciente de sus necesidades actuales, la Implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de vigilancia seleccionados para obtener los niveles de protección esperados; este proceso será liderado de manera permanente por el comité designado para tal fin.

Esta política será revisada con regularidad o cuando se identifiquen cambios en la Entidad, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

La protección y seguridad de los activos de información, parte del concepto fundante de seguridad de la información la cual se desarrolla mediante el principio rector de la gestión de riesgo, y comprende el conjunto de medidas, procedimientos y controles establecidos para el correcto manejo, gestión y control de la información, en todo su ciclo de vida, así como para garantizar sus propiedades fundamentales; la preservación de la confidencialidad, integridad, disponibilidad,

Sociabilidad de la información que se completan con otras participaciones como autenticidad, responsabilidad, trazabilidad y fiabilidad.

Consecuentes de que la seguridad de la información se basa en la presencia de una articulación de políticas que expongan instrucciones claras y sean el soporte tecnológico y legal de la Gerencia General, con el objetivo que estas sean una objeto para la definición de los estándares y procesos internos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES a través de la Oficina de Tecnologías de la Información y las Comunicaciones de la Secretaría de la Secretaria General y Gestión Administrativa, debe asegurar que la información cumpla con los razonamientos de Confidencialidad, Integridad, Disponibilidad, Accesibilidad, Autenticidad, entre otros, mediante el cuidado de datos, la protección frente a accesos no autorizados, el control de acceso a otros sitios web y la adecuada utilización del correo electrónico de la Entidad. Así mismo, proporcionar hardware, software y equipos de comunicaciones en condiciones de seguridad y calidad; realizar revisiones periódicas de seguridad; y garantizar la propiedad de la Información.

El Comité de Seguridad de la Información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES es el garante de formular a la Gerencia General: 1) el compromiso de la implementación del sistema de gestión de seguridad de la información - SGSI, 2) Los lineamientos para la implementación del SGSI, 3) plan de acción anual con las metas, indicadores, actividades, responsables, recursos necesarios. 4) realizar periódicamente las novedades de progresos, en atención a lo antepuesto, se elabora el actual Manual de Gestión de Seguridad de la Información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es el reconocimiento general que representa la postura de la EMPRESA DER SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES con respecto a la resguardo de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la EMPRESA DER SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, velan por la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y divulgación de sus políticas, ordenamientos e instructivos, también la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Garantizar la reserva, integridad y confidencialidad de la información, la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES forma un conjunto de políticas específicas de seguridad y privacidad de la información con alcance a través de los procesos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES para asegurar el direccionamiento estratégico de la Entidad, constituye la afinidad de la política y de los objetivos de seguridad de la información, estos últimos correspondientes a:

a) Disminuir el peligro en las funciones más importantes de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES. b) Verificar los principios de seguridad de la información. c) Efectuar los principios de la función administrativa. d) Conservar la confianza de sus funcionarios, contratistas, empleados y terceros. e) Afirmar la innovación tecnológica. f) Efectuar el sistema de gestión de seguridad de la información. g) Preservar los activos tecnológicos. h) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información. i) Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Alcaldía de Barrancas La Guajira. j) Garantizar la continuidad de los servicios frente a incidentes.

1.1 Nivel de cumplimiento

Nivel de Cumplimiento: Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

1.2 Aplicabilidad: Esta política aplica a toda la entidad **en el proceso de TI**, sus funcionarios, terceros, aprendices, practicantes, proveedores de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES y la ciudadanía en general.

A se establecen las políticas que sobrellevan el plan de seguridad y privacidad de la información de EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

Implementación: La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES ha resuelto **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en objetivos claros alineados a las insuficiencias de la dependencia, y a las exigencias regulatorias que le aplican a su naturaleza.

Responsabilidades: La responsabilidad frente a la seguridad de la información será definida, compartida, publicada y aceptada.

Protección de la Información por accesos otorgados al personal: La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES **protegerá su información** de las amenazas causadas por parte **del personal**.

Protección de la Información por accesos otorgados a terceros: La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos, del riesgo que se genera de los accesos **autorizados a terceros,** como proveedores o clientes, o como resultado de un servicio interno en outsourcing.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Controles para la protección de la Información: EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES **protegerá la información** introducida, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

Control de la operación: La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES **intervendrá en la operación** de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes y bases de datos.

Protección a la Infraestructura Tecnológica La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

Control de Acceso a la Información: La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES **implementará control de acceso** a la información, sistemas y recursos de red.

Incorporación de la Seguridad en los sistemas de información: La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

Mejora continua al modelo de seguridad: La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

Disponibilidad y continuidad de la operación: La EMPRESA DER SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

Cumplimiento de Obligaciones: La EMPRESA DER SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES velara por el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1 Justificación

.

La EMPRESA DER SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES con el fin de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los interesados tanto internos como externos.

La seguridad de la información se deduce como la preservación de las siguientes características:

a) **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b) **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

a) **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

b) **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

c) **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

d) **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

e) **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes 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: excluir 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.

Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

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.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Custodio de activo de información: identifica a un sujeto, un cargo, proceso o grupo de trabajo designado por la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, que posee la responsabilidad de dirigir y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

Datos abiertos: son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

Datos personales sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

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.

Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

***HABEAS DATA*:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Impacto: el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Información: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, *software*, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

Parte interesada (*STAKEHOLDER*): persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Plan de continuidad: plan encaminado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

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

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

Propietario de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

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 consideraciones. (ISO Guía 73:2002).

Responsable del tratamiento: persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento de los datos.

Segregación de tareas: reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Titular de la información: es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociada de modo inequívoco a un individuo o entidad.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

2.2 Objetivo

Definir los mecanismos y todas las medidas necesarias por parte de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES tanto destreza, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.3 Alcance

La Política de Seguridad de la Información para la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES establece las directrices requeridas para implantar el Sistema de Gestión de Seguridad de la Información, definiendo un marco fundamental para diseñar, implementar y operar cualquier requisito normativo, proceso, procedimiento y/o acción, relacionada con la Seguridad de la Información. Esta política se aplica a todos los niveles de la entidad, funcionarios, directivos, asesores, profesionales, técnicos y asistenciales entre otros, así como terceros conformados por proveedores, contratistas, entes de control, entidades adscritas, usuarios internos y externos que accedan o hacen uso de cualquier activo de información independientemente de su ubicación, medio o formato; e inclusive los ex- funcionarios y ex-contratistas, deben mantener la debida confidencialidad sobre la

información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES después de haber terminado la relación contractual.

2.4 Cumplimiento

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES se reserva el derecho de tomar las medidas correspondientes.

2.5 Comunicación

Mediante socialización a todos los funcionarios de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento. La ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en los correos institucionales.

2.6 Monitoreo

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

3. NORMATIVIDAD

El Sistema de Gestión de Seguridad de la Información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES 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. El mensaje de datos es “La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico y demás herramientas tecnológicas que aseguren la gestión informatica.

Ley 594/00 Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones. La presente ley “tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado”. Y “comprende a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley”.

La Ley 850/03 Principio de Transparencia “A fin de garantizar el ejercicio de los derechos, establece en su artículo 9º deberes, instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia”.

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. Se regula el manejo de la información para “todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada”.

Ley 1221 de 2008. Por la cualse establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones. La presente ley tiene por objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC).

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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. Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales. Lineamientos de política para Ciberseguridad y Ciberdefensa. Busca generar lineamientos de política en Ciberseguridad y ciberdefensa encaminados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.

Resolución 2886 de 2012. Por la cual se definen entidades que harán parte de la Red Nacional de Fomento al Teletrabajo y se dictan otras disposiciones. Resolución del Ministerio de Trabajo define "las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo, las actividades que compete desarrollar y su funcionamiento".

Ley 1581/12. Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución…". La ley tiene por objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

Decreto 884 de 2012. Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones. El propósito de la Ley 1221 de 2008 es promover y regular el teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones.

Decreto 2609 de 2012 (hoy incorporado al Decreto Único 1080 de 2015). Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado (Jhon Francisco Cuervo Director Gestión Documental). Sobre la Gestión de Documentos indica que las normas del decreto se aplicarán a cualquier tipo de información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por esta, independientemente del soporte y medio de

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Registro (análogo o digital) en que se produzcan, y que se conservan en: a) Documentos de Archivo (físicos y electrónicos). b) Archivos institucionales (físicos y electrónicos). c) Sistemas de Información Corporativos. d) Sistemas de Trabajo Colaborativo. e) Sistemas de Administración de documentos. f) Sistemas de Mensajería Electrónica. g) Portales, Intranet y Extranet. h) Sistemas de Bases de Datos. i) Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc. j) Cintas y medios de soporte (back up o contingencia). k) Uso de tecnologías en la nube.

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. Serán objeto de inscripción en el Registro Nacional de Bases de Datos, “las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2° de la Ley 1581 de 2012”.

Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública. Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que “Todas las personas tiene derecho a acceder a los documentos públicos salvo los casos que establezca la ley”. El objeto de la ley es “regular el derecho de acceso a la información pública, procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información”.

Decreto 103 de 2015. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. El decreto tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Que para el efecto se hace necesario actualizar el Modelo Integrado de Planeación y Gestión del que trata el Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Decreto 1008 de 14 de Junio de 2018. "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

4. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Generalidades

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

El nivel directivo de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES se compromete a apoyar activamente la seguridad de la información, el cual se verá reflejado en:

4.1 ORGANIZACIÓN DE LA SEGURIDAD

Política

La seguridad de la información debe ser una responsabilidad de la Secretaría General y Gestión Administrativa compartida por todas las dependencias, por lo cual se debe crear un Comité de Seguridad de la Información, integrado por representantes de todas las áreas mencionadas, destinado a garantizar el apoyo manifiesto de la Gerencia General a las iniciativas de seguridad, el mismo contara con un coordinador,

quien cumplirá la función de impulsar la implementación de las Políticas de Seguridad de la Información.

Generalidades

Las Políticas de Seguridad y Privacidad de la Información establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades del área de Tecnología de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

Por esta razón, debe tenerse en cuenta que ciertas actividades de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos, se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Controles

La dirección debe apoyar activamente la seguridad dentro de la entidad con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad y Privacidad de la información.

Las actividades de seguridad y Privacidad de la información deben ser coordinadas por los representantes de todas partes de la entidad con roles y funciones laborales pertinentes, según lo definido en la estructura institucional.

Se deben definir claramente todas las responsabilidades en cuanto a seguridad y privacidad de la información.

Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información.

Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la entidad para la protección de la información.

Se deben mantener contactos apropiados con las autoridades pertinentes

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Contactos adecuados con grupos especiales de interés u otros foros especializados de seguridad o asociaciones profesionales deben ser implementados.

La aproximación de la entidad a la gestión de la seguridad de la información y su implementación debe ser revisada independientemente a intervalos planeados o cuando cambios significativos ocurran en la implementación de la seguridad.

Los riesgos de la seguridad de la información de los procesos de negocio y sus instalaciones de procesamiento, que incluyan a terceras partes deben ser identificados y adicionalmente se deben implementar los controles apropiados antes de permitir el acceso.

Todos los requerimientos de seguridad deben ser atendidos antes de permitir el acceso a los clientes sobre la información o los activos de la entidad.

Los acuerdos con terceros que incluyan el acceso, procesamiento, comunicación o gestión de la información de la entidad o las instalaciones de procesamiento de información, o añadir productos o servicios a las mismas deben cubrir todos los requerimientos de seguridad relevantes.

La Alcaldía debe tener el control de su información previa organización y administración, conforme la definición de su marco gerencial (funciones y responsabilidades).

La oficina de las TIC, debe elaborar los documentos que contengan los lineamientos, guías y procedimientos para organizar, clasificar y valorar la información de la Entidad.

Cada dependencia debe determinar cuál es su información sensible y su disponibilidad.

Todos los usuarios de los recursos informáticos de la entidad deben ubicar la información que necesita ser respaldada en los lugares previamente constituidos para ello; en caso contrario son responsables de sus actos y consecuencias.

La Oficina Jurídica debe verificar que en todos los contratos exista el compromiso de confidencialidad de la información; así como apoyar a la Entidad para que todos los terceros cumplan con la política de seguridad descrita en este documento; y, prestar la asesoría legal de la seguridad de la información necesaria.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.2 INFRAESTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN

Comité de Seguridad de la Información

La seguridad de la información debe ser una responsabilidad de la Secretaría General y Gestión Administrativa compartida por todas las Dependencias, por lo cual se debe crear un Comité de Seguridad de la Información, integrado por representantes de todas las áreas mencionadas, destinado a garantizar el apoyo manifiesto de la Gerencia General a las iniciativas de seguridad. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de las Políticas de Seguridad y privacidad de la Información.

Asignación de Responsabilidades para Seguridad de la Información

El Comité de Seguridad de la Información propondrá a la Gerencia General para su aprobación la definición y asignación de las responsabilidades.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas.

La delegación de la administración por parte de los propietarios de la información debe ser documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

Es responsabilidad del ***Comité de Seguridad de la Información*** de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES la implementación, aplicación, seguimiento y autorizaciones de la política del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

El Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

a) El Alcalde o un delegado especializado,
b) El Secretario de Gobierno y Gestión administrativa o su delegado.
c) El Jefe de la Oficina Asesora de Planeación o su representante.
d) El Jefe de la Oficina Jurídica su delegado.
e) El funcionario encargado de los sistemas de Gestión de Calidad o su delegado
f) El funcionario encargado de la Gestión Documental o su delegado.
g) El Secretario de Hacienda Municipal con funciones de Control Interno o su delegado.
h) El responsable de Seguridad de la información de la entidad.
i) Profesional Especializado con funciones de Planeación o un delegado especializado,
j) Técnico operativo con funciones de almacén.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Este comité deberá revisar y actualizar esta política anualmente presentando las propuestas a la alta dirección para su aprobación.

Estos funcionarios serán los encargados de tratar los temas concernientes a la seguridad de la información, formulando su propio reglamento, en el cual establecerán responsabilidades, funciones y periodicidad de las reuniones. Actuarán como invitados permanentes los Administradores de los diferentes sistemas de información.

El Coordinador del Comité de Seguridad de la Información debe ser el responsable de implementar este ítem.

El responsable del Comité de la Seguridad de la Información tendrá a cargo el mantenimiento de este ítem, ante la máxima autoridad de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad de la información asistirá al personal de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES en materia de seguridad de la información y coordinará la interacción con entidades especializadas.

Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los Responsables de las Dependencias de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, debe ser responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

El Responsable de la Oficina Jurídica, cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

Objetivos del Comité de Seguridad y Privacidad de la Información

El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

Objetivos específicos:

- ✓ Velar por el mejoramiento continuo del MSPI implementado en la entidad.
- ✓ Apoyar el desarrollo de los programas de seguridad y privacidad de la información a través de la gestión/solicitud de recursos en las instancias pertinentes como lo son: Comité de Desarrollo Institucional y Comité Interno de Archivo, Realizar las evaluaciones y seguimiento a las políticas del MSPI para el mejoramiento continuo de las mismas.
- ✓ Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- ✓ Tener conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- ✓ Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

- ✓ Acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información.

- ✓ Garantizar que la seguridad sea parte del proceso de planificación de la información Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

- ✓ Promover la difusión y apoyo a la seguridad de la información dentro de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Coordinar el proceso de administración de la continuidad de las actividades de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

- ✓ Administrar la seguridad de la información dentro de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

- ✓ Fomentar la consulta y cooperación con entidades especializadas para la obtención de asesoría en materia de seguridad de la información.

- ✓ Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información o sistemas de información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

Este Comité tendrá entre sus funciones:

- ✓ Revisar y proponer a la Alta Dirección de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES para su aprobación, las acciones de implementación de las Políticas de Seguridad y Privacidad de la Información y las funciones generales en materia de seguridad de la información.

- ✓ Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

- ✓ Tomar conocimiento, supervisar la implementación y monitoreo de los incidentes relativos a la seguridad.

- ✓ Aprobar las iniciativas más relevantes para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

- ✓ Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

- ✓ Garantizar que la seguridad sea parte del proceso de planificación Institucional.

- ✓ Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos soluciones o servicios.

- ✓ Promover la difusión y apoyo a la seguridad de la información dentro de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Coordinar el proceso de administración de la continuidad del funcionamiento de los sistemas y de la información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES frente a interrupciones imprevistas (Planes de Contingencia).

- ✓ Asignación de un responsable de la seguridad de la información (Oficial de seguridad).

- ✓ Aprobación del documento de políticas de seguridad de la información.

- ✓ Velar por el cumplimiento de las políticas de seguridad de la información.

- ✓ Asignación de responsabilidades asociadas al tema de la seguridad de la información.

Proceso de Autorización para Aplicativos

- ✓ Los nuevos aplicativos deben ser autorizados por los delegados de las Dependencias involucradas, considerando su propósito y uso, conjuntamente con el responsable de Seguridad de la Información, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

- ✓ Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la oficina de las TIC.

- ✓ Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

- ✓ El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso debe ser evaluado en cada caso por la Oficina de las TIC y por el responsable del área al que se destinen los recursos.

Asesoramiento Especializado en Seguridad de la Información

El Responsable de Seguridad de la Información debe ser el encargado de coordinar los conocimientos y las experiencias disponibles en la entidad fin de brindar ayuda en la toma de decisiones en materia de seguridad.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Revisión Independiente de la Seguridad de la Información

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de las Políticas de Seguridad y Privacidad de la Información, a efectos de garantizar que las prácticas de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES reflejen adecuadamente sus disposiciones.

Seguridad frente al Acceso por parte de Terceros

Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la Alcaldía ,el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- ✓ El tipo de acceso requerido (físico/lógico y a qué recurso).
- ✓ Los motivos para los cuales se solicita el acceso.
- ✓ Clasificación de la información.
- ✓ Los controles aplicables a la tercera parte.
- ✓ La incidencia de este acceso en la seguridad de la información de la Alcaldía Municipal de Barrancas.

En todos los contratos, cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, se deben establecer los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

- ✓ Personal de mantenimiento y soporte de hardware y software.

Limpieza, guardia de seguridad y otros servicios de soporte tercerizados.

- ✓ Pasantías y otras designaciones de corto plazo.
- ✓ Consultores e Interventores.

En ningún caso se debe otorgar acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado

los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

- ✓ Cumplimiento de las Políticas de Seguridad y Privacidad de la Información.
- ✓ Protección de los activos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES incluyendo:
  - Procedimientos para proteger los bienes de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES abarcando los activos físicos, la información y el software.
  - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
  - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
  - Restricciones a la copia y divulgación de información.
- ✓ Descripción de los servicios disponibles.
- ✓ Nivel de servicio esperado y niveles de servicio aceptables.
- ✓ Permiso para la transferencia de personal cuando sea necesario.
- ✓ Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
- ✓ Existencia de Derechos de Propiedad Intelectual.
- ✓ Definiciones relacionadas con la protección de datos.
- ✓ Acuerdos de control de accesos que contemplen:
  - Métodos de acceso permitidos, control y uso de identificadores únicos como usuario y contraseñas.
  - Proceso de autorización de accesos y privilegios de usuarios.

- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios, sus derechos y privilegios con respecto a dicho uso.

- ✓ Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- ✓ Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- ✓ Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- ✓ Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- ✓ Proceso claro y detallado de administración de cambios.
- ✓ Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- ✓ Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- ✓ Controles que garanticen la protección contra software malicioso.
- ✓ Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- ✓ Relación entre la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES con contratistas y usuarios.

Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes, seguridad y/o mantenimiento de PC, etc. de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, deben contemplar además de los puntos especificados Tratamiento de la Seguridad dentro de los acuerdos con proveedores8, los siguientes aspectos:

- ✓ Forma en que se cumplirán los requisitos legales aplicables.

- ✓ Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
- ✓ Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.
- ✓ Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES
- ✓ Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres (Contingencia).
- ✓ Niveles de seguridad física que se asignarán al equipamiento tercerizado.
- ✓ Derecho a la auditoría por parte de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES sobre los aspectos tercerizados en forma directa o a través de la contratación.

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

4.3 CLASIFICACIÓN Y CONTROL DE ACTIVOS (GESTION DE ACTIVOS)

Generalidades

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES debe tener total control y conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

Recursos de software: Software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

Activos físicos: equipamiento informático (Servidores, Equipos de Almacenamiento, CPU, monitores, computadores de escritorio, computadoras portátiles, módems), equipos de comunicaciones (routers, PBX, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.

Servicios: servicios informáticos y de comunicaciones, utilitarios generales (iluminación, energía eléctrica normal y regulada, voz, datos, etc.).

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de indicar cómo ha de ser tratada y protegida dicha información.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la entidad.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos.
Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad, disponibilidad y accesibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Inventario de Activos

Se deben identificar los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo debe ser actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 12 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es el Responsable de cada Área Organizativa.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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:

Confidencialidad

0 – Público: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleada de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES o no.

1- Reservada - Uso Interno: Información que puede ser conocida y utilizada por todos los funcionarios de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES y algunas Unidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad, el Sector Público Nacional o terceros.

2 - Reservada - Confidencial: Información que sólo puede ser conocida y utilizada por un grupo de funcionarios, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la entidad, al Sector Público Nacional o a terceros.

3- Reservada - Secreta: Información que sólo puede ser conocida y utilizada por un grupo muy reducido de funcionarios, generalmente de la alta dirección de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros.

Integridad

0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta el funcionamiento de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

1- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la entidad, el Sector Público Nacional o terceros.

2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la entidad, el Sector Público Nacional o terceros.

3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la entidad, al Sector Público Nacional o a terceros.

Disponibilidad:

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

0- Información cuya inaccesibilidad no afecta el funcionamiento de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES

1- Información cuya inaccesibilidad permanente durante un tiempo determinado podría ocasionar pérdidas significativas para la entidad, el Sector Público Nacional o terceros.

2- Información cuya inaccesibilidad permanente durante un tiempo determinado podría ocasionar pérdidas significativas a la entidad, al Sector Público Nacional o a terceros.

3- Información cuya inaccesibilidad permanente durante un tiempo determinado podría ocasionar pérdidas significativas a la entidad, al Sector Público Nacional o a terceros.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, direccionamiento de red, etc.).

Se debe asignar a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en categorías Baja, Media y Alta:

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- ✓ Asignarle una fecha de efectividad.
- ✓ Comunicárselo al depositario del recurso.
- ✓ Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma, identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

En adelante, en este documento, se mencionará como “información clasificada” (o “datos clasificados”) a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

Controles

- ✓ La oficina de las TIC, debe documentar el procedimiento de clasificación de la información como activo de la Entidad, el cual debe prevalecer los principios de la información en las cuales se basa la seguridad como son confidencialidad, integridad y disponibilidad.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Todas las dependencias de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES deben clasificar la información y determinar su sensibilidad y criticidad en los equipos informáticos.

- ✓ Los funcionarios encargados de la información deben clasificar la información de acuerdo con su grado de sensibilidad y criticidad, así como de documentar y mantener actualizada la clasificación, los permisos de acceso a los sistemas de información.

- ✓ Todos los funcionarios deben clasificar, supervisar, proteger y restringir accesos a la información generada en el ejercicio de sus funciones.

- ✓ La oficina de las TIC debe apoyar al responsable de elaborar el inventario de sus activos importantes y/o asociados a cada uno de los sistemas de información; y, luego consolidar en un solo inventario dicha información.

- ✓ La oficina de las TIC, debe anualmente revisar el inventario de sus activos importantes y/o asociados a cada uno de los sistemas de información o cuando exista un cambio que afecte el inventario unificado.

4.4 POLÍTICA DE RESPALDO DE INFORMACIÓN

Política

La Oficina de las Tic implementará mecanismos para el almacenamiento seguro y protección de la información en medios magnéticos o electrónicos, perpetuarla y garantizar su recuperación en caso de fallas de los equipos de cómputo u ocurrencia de eventos de contingencia o situaciones fortuitas.

Los respaldos de información (backups) de valor o sensible debe tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.

El área dueña de la información en conjunto con la oficina Asesora de Planeación y Oficina de las Tic, definirá la estrategia a seguir para el respaldo de la información.

La información y datos de los aplicativos de misión crítica deben ser almacenados bajo un esquema estructurado de backup, que incluya almacenamiento en discos duros externos, en sitios externos a la entidad y con verificación periódica de su restauración.

Se debe utilizar una utilidad de copias de seguridad para programarlas, teniendo en cuenta la fecha, la hora, la frecuencia y el recurso de red donde se realiza la configuración.

Las copias de seguridad son programadas dependiendo la periodicidad de los cambios realizados en las aplicaciones (códigos fuentes, bases de datos, configuración del sistema).

Toda la información contable, de propiedad intelectual y de propiedad de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES debe ser conservada de acuerdo con las normas de ley vigentes.

Todos los medios físicos donde la información de valor y crítica sea almacenada deben tener un control de acceso y custodia para evitar su pérdida o acceso no autorizado.

Los funcionarios públicos son responsables de los respaldos de su información en los computadores asignados.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Controles

- ✓ La realización de copias de respaldo debe ser acorde al procedimiento para copias de seguridad de los sistemas de información establecido en la empresa, lo cual permitirá garantizar la oportuna recuperación de la información en la eventualidad que ocurra algún percance.

- ✓ Se debe mantener las copias de seguridad de la información según la periodicidad establecida en el procedimiento de backups y proveer de un lugar externo a las instalaciones de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES la cual permita recuperar la información en caso de una contingencia.

- ✓ La custodia de las copias de respaldo de la información se realizará externamente con una compañía de seguridad especializada en este tema, contratada por la empresa.

- ✓ Es responsabilidad de la Oficina de las Tic, verificar mensualmente que se hayan realizado todas las copias de seguridad de la información almacenada en cada equipo y que estas se encuentren en buen estado para su almacenamiento y posterior restauración.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Al final de cada año, la Oficina de las Tic, guardará una copia de seguridad de toda la información almacenada en la vigencia, en medios magnéticos, para su conservación y custodia.

- ✓ La Oficina de las Tic deberá garantizar la privacidad y confidencialidad de la información en aquellas áreas que la soliciten mediante el manejo de claves de seguridad y el encriptamiento de la información.

- ✓ Se debe informar a la oficina asesora de comunicaciones y sistemas del retiro de funcionarios o contratistas que manejen contraseñas, permisos de usuarios ó claves de seguridad cuando estos finalicen su contrato o terminen labores con la empresa, desactivar las cuentas de usuario, claves, contraseñas, permisos y similares, dentro de los sistemas de información de la empresa.

- ✓ Los dispositivos o medios que contengan copias de seguridad (backups) deberán mantenerse almacenados en un lugar seguro previamente definido por la Oficina de las Tic y su manejo será exclusivo de dicha área.

- ✓ Los funcionarios, contratistas y terceros responsables de la infraestructura, sistemas de información y bases de datos requeridos para la operación de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES deberán generar las respectivas copias de respaldo, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido en la presente política.

- ✓ Los encargados de las copias de respaldo deben velar porque la información sea almacenada conforme a los lineamientos establecidos, es decir, de forma controlada y según las necesidades de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES Así mismo deberán realizar una prueba periódica de las copias con el fin validar el correcto funcionamiento y la efectiva restauración.

- ✓ Los dueños de los procesos o activos de información, serán los encargados de velera por que las copias se realicen de acuerdo con lo establecido y que las mismas se ajusten a las necesidades y requerimientos, garantizando el cumplimiento de los objetivos estratégicos y misionales de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES

- ✓ Los funcionarios, contratistas y terceros de la Alcaldía de Barrancas deberán almacenar la información requerida para sus procesos operativos, dentro del servidor de almacenamiento provisto por la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES con el fin de garantizar la disponibilidad y copias de respaldo de cada una de las áreas. Así mismo serán responsables de depurar la información para la optimización de los recursos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ La información requerida en el desarrollo de las operaciones orientadas al cumplimiento de los objetivos estratégicos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, deberá tratarse conforme a los lineamientos legales, técnicos y administrativos determinados conforme a las tablas de retención documental, la gestión de riesgos, así como a los niveles de clasificación de la información.

- ✓ Los tiempos de preservación de las copias de respaldo de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES se definirán según los requerimientos técnicos, administrativos y jurídicos, y se determinarán por parte de la entidad los recursos requeridos para acceso y validación de la información contenida durante los tiempos previstos.

- ✓ La solicitud de respaldo deberá presentarse formalmente al responsable de las copias de respaldo, determinando las necesidades, la información sujeta al respaldo, periodos, niveles de clasificación de la información y el tiempo de retención de las copias. Así mismo, se realizarán las respectivas pruebas de funcionamiento conforme a los propósitos para los cuales han sido recaudadas.

- ✓ Los funcionarios encargados de las copias de respaldo, velarán para que durante su transporte y custodia, la misma no sea manipulada por personas no autorizadas.

- ✓ Las copias de respaldo deberán ser almacenadas en lugares que tengan los debidos controles de seguridad físicos y tecnológicos, esto es, que permitan limitar el acceso sólo a las personas autorizadas y garanticen la disponibilidad de la información. A su vez, deberán registrarse todas las actividades desarrolladas frente al tratamiento y manipulación de las copias para guardar la trazabilidad.

- ✓ Cumplido el tiempo requerido de almacenamiento de las copias de respaldo, se deberá proceder a su destrucción o eliminación, asegurando que la información contenida no sea accedida por personas no autorizadas. Las actividades realizadas deberán ser registradas para su posterior consulta.

4.5 USO DE DISPOSITIVOS MÓVILES

Cuando se utilizan dispositivos móviles, se debe tener especial cuidado en garantizar que no se comprometa la información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Tablets, Ipads, Laptops o PDA, (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, USBs, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), cámaras digitales, etc.

Controles

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo pérdida, robo o hurto. En consecuencia, deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- ✓ Existirán redes segmentadas con los controles establecidos por la Secretaría General y Gestión Administrativa, para que los funcionarios, contratistas y terceros puedan acceder al recurso, manteniendo la seguridad de los activos de información de la Alcaldía Municipal de Barrancas.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Se deberán proteger física y lógicamente los dispositivos móviles propiedad de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES con el fin de evitar el hurto, acceso o la divulgación no autorizada de la información. En caso de ser necesario, se cifrará la información y se tendrán copias de respaldo.

- ✓ La Secretaría de la Gobierno y Gestión Administrativa, con la información suministrada por el Secretaría de la Función Pública, brindará o denegará a los funcionarios, contratistas y terceros el acceso a la información o sistemas de información a través de los dispositivos móviles conforme los roles y responsabilidades.

- ✓ En caso de extravió o hurto de un dispositivo móvil asignado por la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES el funcionario, contratista o tercero será el responsable de informar el hecho de manera inmediata a la entidad y a su vez al Oficial de Seguridad de la Información, con el propósito de establecer de las medidas de seguridad adecuadas y oportunas para la protección de la información contenida.

    - o Permanecer siempre cerca del dispositivo.
    - o No dejar desatendidos los equipos.
    - o No llamar la atención acerca de portar un equipo valioso.
    - o No poner identificaciones de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES en el dispositivo, salvo los estrictamente necesarios.
    - o No poner datos de contacto técnico en el dispositivo.
    - o Mantener cifrada la información clasificada.

- ✓ Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la Alcaldía Municipal de Barrancas, los que incluirán:

    - o Revocación de las credenciales afectadas
    - o Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

4.6 COMPUTADORES, PORTATILES, SERVIDORES

Políticas

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones.

Los computadores de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

Controles

- ✓ El equipo de cómputo será asignado de acuerdo al puesto o función laboral en su área de trabajo. Siendo el responsable de dicha asignación el Jefe del área.
- ✓ Cada equipo está preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.
- ✓ En caso de presentar una falla física o lógica se deberá notificar al área de Informática y en el caso de ser requerido enviar el equipo para su revisión y/o reparación de acuerdo al procedimiento establecido.
- ✓ En ningún caso el usuario intentará reparar el equipo ó diagnosticarlo, únicamente debe informar de la posible falla.
- ✓ El usuario será el único responsable del equipo de cómputo.
- ✓ En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.
- ✓ Solo se utilizará el equipo para funciones de interés del área y de ninguna manera para asuntos personales.
- ✓ El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo del equipo de cómputo y periféricos básicos.
- ✓ En caso de que el usuario no tenga conocimientos y/o experiencia, se notificará al área de sistemas para su correspondiente capacitación.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- La adquisición de equipo será con cargo al presupuesto de cada área o de la secretaria general, las características técnicas serán proporcionadas por el área de sistemas.

- La solicitud del equipo de cómputo será responsabilidad del área interesada, bajo las características técnicas definidas por el área de sistemas e informando a las áreas relacionadas con la asignación de los recursos.

- Toda recepción de equipo de cómputo por adquisición o donación se realizará a través del Área de Inventarios, con el apoyo del área de sistemas.

- La salida de equipo de cómputo del Almacén, será total responsabilidad del almacén, el cual revisará la integridad física y el área de sistemas instalará la integridad lógica e instalará y preparará el software y hardware correspondiente a las licencias contenidas.

- Cada equipo contiene el software de acuerdo a las necesidades del área de trabajo, El cual No deberá ser alterado.

- Por ningún motivo el usuario instalará software de promoción y/o entretenimiento.

- La adquisición o desarrollo de software será responsabilidad del área de sistemas.

- El usuario deberá reportar de forma inmediata a la Oficina de las Tic cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, contactos eléctricos con riesgo de incendio u otros.

- El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

- Es responsabilidad del usuario evitar en todo momento la fuga de la información de la institución que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

- Cualquier persona que tenga acceso a las instalaciones de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, deberá registrar al Momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Institución, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la autorización de salida del área de Inventarios anexando el vale de salida del equipo debidamente por el secretario de la oficina o la equivalente en las dependencias de la entidad.

- Los centros de cómputo u oficina de servidores de la Institución son áreas restringidas, por lo que sólo el personal autorizado por las Oficina de las Tic puede acceder a ellos.

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Oficina de las Tic, en caso de requerir este servicio deberá solicitarlo atreves de la mesa de ayuda.

- El Área de Almacén será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Oficina de las Tic.

- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la institución.

- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

- Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro en el servidor o equipo, o en su defecto en la carpeta “Mis Documentos” ya que las otras están destinadas para archivos de programa y sistema operativo.

- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.

- Se debe mantener el equipo informático en un entorno limpio y sin humedad.

- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al área de Sistemas a través de un plan detallado o una solicitud para el debido acompañamiento de la oficina de las Tic.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Queda prohibido que el usuario abra o desarme los equipos de cómputo.
- ✓ Únicamente el personal autorizado por la Oficina de las Tic y Calidad podrá llevar a cabo los servicios y reparaciones al equipo informático.
- ✓ El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- ✓ El usuario deberá dar aviso inmediato a la Oficina de las Tic, y Almacén de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.
- ✓ El uso de los grabadores de discos externos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- ✓ El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se les dé.
- ✓ El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad.
- ✓ Los equipos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- ✓ Debe respetarse y no modificar la configuración de hardware y software establecida por la Oficina de las Tic.
- ✓ Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el bloqueo de pantalla para que se active al cabo de 30 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además, el usuario debe activarlo manualmente cada vez que se ausente de su oficina.
- ✓ Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.
- ✓ Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la entidad está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- ✓ Los usuarios no deben copiar a un medio removible (como una USB), el software o los datos históricos residentes en las computadoras de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, sin la aprobación previa del área de sistemas o del jefe inmediato.

- ✓ No pueden extraerse datos fuera de la entidad sin la aprobación previa de la Administración. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

- ✓ Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a la Oficina de las Tic y poner el computador en cuarentena hasta que el problema sea resuelto.

- ✓ Sólo pueden descargarse archivos de redes externas de acuerdo a los procedimientos establecidos.

- ✓ Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otras dependencias de la entidad.

- ✓ No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por la Oficina de las Tic.

- ✓ Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por la Oficina de las Tic.

- ✓ Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

- ✓ No deben usarse USB u otros medios de almacenamiento en cualquier computador de la institución a menos que se haya sido previamente verificado que están libres de virus u otros agentes dañinos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Periódicamente debe hacerse el respaldo de los datos guardados en computadores y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de la entidad deben guardarse en otra sede, lejos del edificio.

- ✓ Los usuarios de computadores son responsables de proteger los programas y datos contra pérdida o daño.

- ✓ El área de sistemas será responsable de la generación de las copias de seguridad de los equipos de la entidad y definirá la frecuencia del respaldo.

- ✓ Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la entidad.

- ✓ No debe dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la entidad.

- ✓ El personal que utiliza un computador portátil que contenga información confidencial de la entidad, no debe dejarlo desatendido, sobre todo cuando esté de viaje.

- ✓ Todos los equipos permanecerán en el lugar registrado por el área de almacén.

- ✓ Solo los equipos portátiles de propiedad de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES podrán desplazarse con previa autorización del responsable de la dependencia y bajo la responsabilidad total del usuario.

- ✓ Toda actividad que se realice por terceros en las áreas de servidores y de procesamiento debe ser supervisada por el responsable de la dependencia.

- ✓ El jefe de la dependencia o Secretarias mantendrá un registro de todas las personas ajenas que ingrese a las áreas de servidores y de procesamiento de información, indicando, fecha, hora, nombre, actividad realizada, y nombre de quien autorizó.

- ✓ Las Instalaciones de procesamiento de información administradas por la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES encontrarán separadas de las administradas por terceros.

- ✓ Se debe impedir el ingreso a las áreas restringidas, de equipos de cómputo móvil, fotográfico, videos, dispositivos removibles o cualquier otro equipo que registre información, a menos que sea autorizado por el responsable de dicha área.

- ✓ Está prohibido fumar, beber o consumir alimentos en las áreas de servidores o cercanas a las estaciones de trabajo.

- ✓ No está autorizado almacenar material peligroso, combustible e inflamable en sitios cercanos a las áreas de procesamiento o almacenamiento de información.

- ✓ **Ubicación de Servidores:** Los servidores estarán ubicados en un área física que cumpla con las siguientes medidas de seguridad:

    - El acceso debe ser restringido a personal autorizado
    - La temperatura debe ser la adecuada para la cantidad de equipos
    - Debe tener protección contra descargas eléctricas
    - El mobiliario debe ser el adecuado
    - Ubicación física en sitio libre de daño por humedad, goteras, inundaciones y demás efectos del clima.

- ✓ **Funcionalidad y mantenimiento de Servidores:** Todo servidor que proporcione servicios a través de la red debe:

- ✓ Funcionar las 24 horas al día los 365 días del año
- ✓ Tener mantenimiento preventivo mínimo dos veces al año
- ✓ Ser objeto de Mantenimiento semestral donde se realizara la depuración de bitácoras
- ✓ Hacerle revisión de su configuración anual
- ✓ Ser Monitoreado diariamente por la persona encargada o director del Grupo de Informática
- ✓ La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES debe garantizar la seguridad física en todas las secretarías de la Entidad para prevenir e impedir accesos no autorizados, daños e interferencia a las instalaciones así como a la información que recibe y genera la entidad.
- ✓ Todos los recursos físicos inherentes a los sistemas de información de La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES como las instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc. deben estar protegidos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Los recursos informáticos utilizados para el procesamiento de la información deben estar ubicados en sitios estratégicos con mecanismos de seguridad que permita controlar el acceso solo a las personas autorizadas e incluir en la protección de los mismos los traslados por motivos de mantenimiento u otros escenarios.
- ✓ La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES a través de las diferentes dependencias debe identificar y garantizar el control de los aspectos ambientales que pueden llegar a interferir el correcto funcionamiento de los recursos tecnológicos inherentes en el procesamiento y almacenamiento de la información institucional.

- ✓ Se deben definir los niveles de seguridad física en las instalaciones de sus oficinas que está bajo su responsabilidad y como encargados del procesamiento de la información son los encargados de aprobar o negar la autorización formal del acceso a las oficinas de su competencia cuando sea requerido.
- ✓ Todos los funcionarios de la Entidad son responsables del uso adecuado de las pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario que realiza.
- ✓ Toda actividad que se realice por terceros en las áreas de servidores y de procesamiento debe ser supervisada por el responsable de la Dependencia.

- ✓ El jefe de la Dependencia o Secretaria mantendrá un registro de todas las personas ajenas que ingrese a las áreas de servidores y de procesamiento de información, indicando, fecha, hora, nombre, actividad realizada, y nombre de quien autorizó.

- ✓ Las Instalaciones de procesamiento de información administradas por la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES se encontrarán separadas de las administradas por terceros.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Se debe impedir el ingreso a las áreas restringidas, de equipos de cómputo móvil, fotográfico, videos, dispositivos removibles o cualquier otro equipo que registre información, a menos que sea autorizado por el responsable de dicha área.

- ✓ El usuario deberá reportar de forma inmediata a la Oficina de las Tic cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

- ✓ El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

- ✓ Es responsabilidad del usuario evitar en todo momento la fuga de la información de la institución que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

- ✓ Cualquier persona que tenga acceso a las instalaciones de la institución, deberá registrar al Momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

- ✓ Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones de la Alcaldía Municipal únicamente con la autorización de salida del área de Almacén anexando el vale de salida del equipo debidamente por el secretario de la oficina o la equivalente en las dependencias de la entidad.

- ✓ Los usuarios deberán asegurar que toda la información que desean sea respaldada se deberá guardar en los servidores de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES ya que el Área de sistemas no se hace responsable por perdidas de información que no se encuentren dentro del servidor.

- ✓ En caso de que haya pérdida de información dentro del servidor podrán recuperar su información solicitándolo con un incidente indicando el nombre del archivo y la ruta del mismo para poder encontrarlo dentro del sistema de respaldos.

  El área donde están ubicado los servidores de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES es un área restringida, por lo que sólo el personal autorizado por el Sistemas puede acceder a ellos.

- ✓ Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Oficina de las Tic, en caso de requerir este servicio deberá solicitarlo.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ El Área de Almacén será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Oficina de las Tic.

- ✓ El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la entidad.

- ✓ Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

- ✓ Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro en el servidor o en mis “Mis Documentos” ya que las otras están destinadas para archivos de programa y sistema operativo.

- ✓ Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

- ✓ Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- ✓ Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación a la Oficina de las Tic a través de un plan detallado.
- ✓ Queda prohibido que el usuario abra o desarme los equipos de cómputo.
- ✓ Únicamente el personal autorizado por la Oficina de las Tic podrá llevar a cabo los servicios y reparaciones al equipo informático.
- ✓ Los usuarios deberán asegurarse de respaldar en el servidor la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.
- ✓ El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- ✓ El préstamo de laptops tendrá que solicitarse en la Oficina de las Tic, con el visto bueno del Secretario de las dependencias de la entidad.
- ✓ El usuario deberá dar aviso inmediato a la Oficina de las Tic, y el área de Almacén de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.
- ✓ El uso de los grabadores de discos compactos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- ✓ El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se les dé.
- ✓ Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el Oficina de las Tic.
- ✓ El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad
- ✓ Los equipos de la compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- ✓ Debe respetarse y no modificar la configuración de hardware y software establecida por el Oficina de las Tic

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

- ✓ Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder interrumpibles (UPS).

- ✓ Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

- ✓ Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 30 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

- ✓ Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

- ✓ Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

- ✓ Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Compañía.

- ✓ A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- ✓ Los usuarios no deben copiar a un medio removible (como una USB), el software o los datos residentes en las computadoras de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, sin la aprobación previa de la gerencia.

- ✓ No pueden extraerse datos fuera de la entidad sin la aprobación previa del Secretario. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

- ✓ Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner el computador en cuarentena hasta que el problema sea resuelto.

- ✓ Sólo pueden descargarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otras dependencias de la entidad.

- ✓ No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Oficina de las Tic.

- ✓ Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por la Oficina de las Tic.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

- ✓ No deben usarse USB u otros medios de almacenamiento en cualquier computador de la institución a menos que se haya sido previamente verificado que están libres de virus u otros agentes dañinos.

- ✓ Periódicamente debe hacerse el respaldo de los datos guardados en computadores y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de la entidad deben guardarse en otra sede, lejos del edificio.

- ✓ Los usuarios de computadores son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de las distintas dependencias son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

- ✓ La información de la institución clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Oficina de las Tic.

- ✓ No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

- ✓ El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

- ✓ Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la entidad.

- ✓ No debe dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la entidad.

- ✓ El personal que utiliza un computador portátil que contenga información confidencial de la entidad, no debe dejarlo desatendido, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

4.7 USO DE INTERNET

Políticas

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Controles

- ✓ El acceso a internet deberá encontrarse protegido por filtros para disminuir sitios peligrosos que contengan códigos maliciosos o que se encuentren ajenos al servicio, Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.
- ✓ No navegar por sitios no confiables.
- ✓ Se prohíbe el uso de sitios de radios online a excepción de sitios institucionales.
- ✓ Se prohíbe el uso de intercambio de archivos a través de sistemas o programas de internet, sin que estos cuenten con la debida acreditación y controles de seguridad.
- ✓ Se prohíbe el uso de sitios de chat (Messenger, chat, etc.), a menos que este sea de uso institucional.
- ✓ Se prohíbe el uso de internet para actividades ilícitas.
- ✓ Se prohíbe la descarga que no cumpla con la normativa vigente de copyright y similar.
- ✓ Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.
- ✓ No compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo)

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ No permitir que el navegador de internet recuerde la contraseña automáticamente.
- ✓ Evitar participar en juegos de entretenimiento en línea.
- ✓ Si no está navegando por internet, cierre todas las ventanas abiertas.
- ✓ Los canales de acceso a internet de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES no podrán ser usados para fines diferentes a los requeridos en el desarrollo de las actividades propias de los cargos. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.
- ✓ No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Alcaldía o de las personas.
- ✓ La Alcaldía de Barrancas se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.
- ✓ El uso de Internet para la revisión de correo electrónico personal, en cumplimiento de actividades propias de la Entidad, está autorizado siempre y cuando se observen los mismos lineamientos estipulados para la utilización del servicio de correo interno.
- ✓ Está terminantemente prohibido usar la red corporativa de internet para consultar, divulgar o promover lugares en Internet con contenido erótico, pornográfico, Intolerancia (racial, político), religioso, juegos virtuales, violencia, uso de drogas o lugares donde se use lenguaje soez.
- ✓ Está prohibido el uso del internet para el manejo de cuentas personales de acceso a correos, redes sociales como: Facebook, sónico, twiter, msn, google, twitter, entre otras y servicios de chat externos, con excepción de los autorizados por la Oficina de las Tic para manejo institucional.
- ✓ El sistema de correo electrónico debe ser usado únicamente para el ejercicio de las funciones corporativas de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas o terceros.
- ✓ La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, la entidad realizará las revisiones y/o auditorias respectivas directamente o a través de terceros.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES

- ✓ Los funcionarios públicos, contratistas y personal temporal que hayan recibido aprobación para tener acceso a Internet a través de los recursos informáticos de la Entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

- ✓ Sólo deben imprimirse los mensajes importantes que así lo requieran, ya que una de las ventajas y fines del servicio de Correo Electrónico Institucional es la transmisión de información con ahorro de papel.

- ✓ Utilizar el servicio de internet exclusivamente para fines laborales.
- ✓ Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas o practicantes con acceso a este servicio.
- ✓ Tomar las medidas de precaución necesarias al descargar documentos para evitar el acceso de virus en las redes y equipos informáticos.
- ✓ Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.
- ✓ Si requiere navegar en algún sitio bloqueado se deberá solicitar a la Oficina de las Tic.

4.8 MANEJO DE REDES SOCIALES

Políticas

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES con el fin definir las pautas generales para asegurar una adecuada protección de la información y un adecuado manejo, en el uso las redes sociales, por parte de los usuarios autorizados.

Controles

- ✓ En lo posible la Entidad deberá bloquear todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiera acceder a ellos, deberá enviar la solicitud formal al área de sistemas.
- ✓ Solo podrán tener acceso a redes sociales un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.
- ✓ La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES que sea creado a nombre personal, como redes sociales, twitter®, facebook®, youtube® likedink® o blogs, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

4.9 MANEJO DE IMPRESORAS

Políticas

Estas políticas son necesarias con el fin de asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Controles

- Los documentos que se impriman en las impresoras de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES deben ser de carácter institucional.

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la mesa de ayuda de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES

  MANEJO APROPIADO DE CONTROL DE VIRUS Políticas La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES con el fin Definir las pautas generales para asegurar una adecuada protección de la información y un adecuado manejo de los equipos, establece los lineamientos a seguir para proteger los activos de la entidad contra amenazas informáticas.

Controles

- ✓ La Entidad deberá definir un producto estándar licenciado entorno de sus estaciones de trabajo, resguardando el correcto funcionamiento de los equipos computo.

- ✓ El sistema de actualizaciones y detección diaria deberá estar automatizado.

- ✓ Se debe comunicar de cualquier infección por virus que no fue eliminada por el antivirus, al área de sistemas.

- ✓ Los usuarios no podrán desinstalar o cambiar el producto de antivirus existente en su equipo.

- ✓ Los dispositivos extraíbles, antes de ser usados deben ser escaneados con el antivirus.

4.10 SWITCHES Y ROUTERS

Política

La Oficina de las Tic es absolutamente responsable del manejo de los dispositivos de red entiéndase por Routers y Switches de los que dispone la institución, velando porque estén dispuestos en lugares seguros y protegidos a nivel físico, así como también a nivel lógico.

Controles

- ✓ Las contraseñas predefinidas que traen los dispositivos nuevos, deben cambiarse inmediatamente al ponerse en servicio el dispositivo.
- ✓ Se deberá designar al personal que efectuará las actividades de instalación, desinstalación, mantenimiento y conexión física de estos dispositivos.
- ✓ Definir procedimientos de recuperación ante eventualidades físicas.
- ✓ Definir procedimientos de respuesta, autoridades y los objetivos de la respuesta después de un ataque exitoso, incluir esquemas de preservación de la evidencia.
- ✓ Se deberán enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
- ✓ Se deberán identificar los servicios de configuración dinámica de los Routers, y las redes permitidas para accesar a dichos servicios
- ✓ Se deben tener plenamente identificados los protocolos de ruteo a utilizar, y los esquemas de seguridad que proveen Seguridad en el Router

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.11 CORREO ELECTRÓNICO INSTITUCIONAL

Política

El correo electrónico es de carácter personal e intransferible, es deber de cada uno de los usuarios mantener el uso de este y de su contraseña siguiendo estas dos premisas y por ningún motivo se debe permitir a otra persona fuera de su dependencia acceder a este recurso. Todo esto para facilitar la comunicación entre funcionarios y terceras partes. Por este motivo la alcaldía municipal de Calarcá proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

El uso de la Internet estará restringido en concordancia con las políticas de seguridad informática de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, Desde la Oficina de las Tic se administrarán todos los accesos a Internet de los funcionarios que lo necesiten, evitando de esta forma colapsar el servicio. El usuario que sea sorprendido según el reporte diario del web máster visitando sitios no autorizados por la empresa, en primera instancia se le hará el llamado de atención y si reincide se informara a la oficina de control interno disciplinario para personal de planta o si es un contratista se informará a la oficina de Talento Humano para que informe a la empresa que presta los servicios.

Controles

- ✓ Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- ✓ El Correo electrónico institucional es de uso exclusivo para actividades relacionadas con la Entidad y queda restringido el uso para otros fines.

- ✓ Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.

- ✓ La contraseña de correo debe ser cambiada periódicamente e informar de la nueva contraseña al área de sistemas.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ No abrir link sospechoso llegados por correos electrónicos (bancos, tiendas, etc.).
- ✓ No completar datos personales en correos electrónicos sospechosos.
- ✓ Eliminar periódicamente los correos no deseados (spam o sospechoso).
- ✓ Los accesos a la red (Internet) serán solo de interés laboral y no personal. Se establecen horarios de uso a fin de no saturar el canal y poder hacer un buen uso del mismo.
- ✓ Las páginas de consulta común por su contenido de interés general y de carácter laboral como: DANE, DAFP, presidencia, notinet, soi, secop 1 y 2 Gobierno Digitaletc. Se pueden consultar en cualquier momento dentro del horario laboral.
- ✓ De ninguna manera se podrá acceder a páginas de entretenimiento, pornografía o fuera del contexto laboral.
- ✓ El usuario no deberá bajar (ó copiar) archivos sospechoso o con extensiones desconocidas de la red sin autorización de la Oficina de las Tic.
- ✓ La comunicación estará limitada por las políticas de seguridad de la Oficina de las Tic.
- ✓ Solo se enviará y recibirá información de interés laboral.
- ✓ En ningún caso de recibir información en archivos adjuntos de dudosa procedencia o que no esté esperando, se notificará a la Oficina de las Tic, para analizar y evitar que ingresen virus al sistema.
- ✓ Al enviar información el responsable será el usuario correspondiente.
- ✓ No se deberá enviar información de tipo estadístico, informativo o información relevante de las acciones de la Dirección, Área de trabajo o de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES a ningún destino no autorizado.
- ✓ Se tienen correos institucionales dentro de la política de austeridad en el gasto público, se recomienda su uso para toda la comunicación interna y ahorrar tinta y papel, igualmente las carpetas compartidas por la LAN para mover y compartir información.
- ✓ El uso de Internet está limitado por las políticas de seguridad de la Oficina de las Tic.
- ✓ Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más

(mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la institución, a menos que cuente con la autorización del departamento de informática.

- ✓ Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- ✓ Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones

- ✓ Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

- ✓ Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

- ✓ El correo electrónico institucional no se deberá utilizar para enviar mensajes como cadenas o mensajes con contenido censurable. En general el correo electrónico institucional es de uso empresarial y no personal.

- ✓ Se debe eliminar periódicamente los mensajes del correo electrónico institucional para no llegar al límite establecido por la Oficina de las Tic, porque el sistema bloquea el buzón de correo una vez se ha excedido el límite. El tamaño del límite de capacidad del buzón del correo electrónico institucional depende de las necesidades de cada funcionario o contratista.

- ✓ Se debe almacenar en el disco duro los documentos importantes que fueron recibidos por el correo electrónico institucional, teniendo en cuenta que el buzón de correo electrónico es un sitio de intercambio de información mas no un sitio de almacenamiento de información. Una vez almacenado en el disco duro debe ser eliminado del correo.

- ✓ Está terminantemente prohibido usar la red corporativa de internet para consultar, divulgar o promover lugares en Internet con contenido erótico, pornográfico, Intolerancia (racial, político), religioso, juegos virtuales, violencia, uso de drogas o lugares donde se use lenguaje soez.

- ✓ Está prohibido el uso del internet para el manejo de cuentas personales de acceso a correos, redes sociales como: facebook, sónico, twiter, msn, google+, twitter, entre otras y servicios de chat externos, con excepción de los autorizados por la Oficina de las Tic para manejo institucional.

4.12 SEGURIDAD DE RECURSOS HUMANOS

- ✓ La oficina asesora de las TIC, debe documentar los lineamientos de seguridad que contribuya a reducir los posibles riesgos que el ser humano pueda cometer voluntaria o involuntariamente; que incluye el uso adecuado de instalaciones y recursos tecnológicos para la seguridad de la información.

- ✓ La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES a través de su secretaría general debe informar al personal nuevo que se vincule o contrate en la Entidad la existencia del Manual de Políticas de Seguridad y Privacidad de la información e incluir en los contratos de estos últimos, el compromiso de confidencialidad de la información y la responsabilidad en materia de seguridad.

- ✓ La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES debe capacitar permanentemente a los funcionarios en materia de seguridad de la información y difundir las posibles amenazas y riesgos que afectan los recursos informáticos de la Entidad.

- ✓ La Oficina de las TIC, debe realizar permanentemente campañas de seguridad de la información establecidas en el plan de sensibilización, capacitación y comunicación. Estas actividades del plan van dirigidas a todos los usuarios de los recursos informáticos para evitar que realicen tareas inseguras que conlleven a pérdida y destrucción de información y/o activos informáticos en la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

- ✓ En los correos institucionales se encuentra el documento Plan de Sensibilización, Capacitación y Comunicación a disposición de la comunidad en general, con el fin de facilitar el acceso a la información respectiva.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.13 BASES DE DATOS

Política

Es obligación de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES y en especial del administrador de la base de datos controlar todo tipo de manejo que se efectué sobre la base de datos y velar por mantenerla protegida contra todo tipo de ataque daño o intrusión sean de naturaleza externa o interna, y en caso de presentarse este tipo de situaciones deben aplicarse los procedimientos correctivos necesarios para restaurar el funcionamiento de la misma sin que ocurra perdida de información.

Es política de la entidad prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras entidades o personas y que le haya sido confiada.

Controles

- ✓ Es función del administrador especificar los privilegios que un usuario tiene sobre la base de datos La base de datos debe estar protegida contra el fuego, el robo y otras formas de destrucción.
- ✓ Se debe garantizar que los datos sean reconstruidos en caso de daño, efectuando periódicamente un respaldo de la información
- ✓ Los datos deben poder ser sometidos a procesos de auditoria. La falta de auditoria en los sistemas de computación ha permitido la comisión de grandes delitos.
- ✓ El sistema debe diseñarse a prueba de intromisiones. Los programadores, por ingeniosos que sean, no deben poder pasar por alto los controles.
- ✓ El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas. Las acciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.
- ✓ Se deberá demorar la respuesta de la base de datos ante claves erróneas aumentando la demora cada vez y se alertara si hay demasiados intentos.

- ✓ Registrar todas las entradas cada vez que un usuario entra, se debe chequear cuándo y desde dónde entró la vez anterior.

- ✓ Hacer chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo, cuando usuario está de vacaciones).

- ✓ Identificar y autorizar a los usuarios: uso de códigos de acceso y palabras claves, exámenes, impresiones digitales, reconocimiento de voz, barrido de la retina, etc.

- ✓ Se deberá contar con un sistema de manejo de autorizaciones con el fin de usar derechos de acceso dados por el terminal, por la operación que puede realizar o por la hora del día.

- ✓ Uso de técnicas de cifrado para proteger datos en la base de datos

- ✓ Manejo de la tabla de usuarios con código y contraseña, control de las operaciones efectuadas en cada sesión de trabajo por cada usuario y anotadas en la bitácora, lo cual facilita la auditoría de las bases de datos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.14 RED LAN

Política

Será considerado como un ataque a la seguridad y una falta grave, cualquier actividad no autorizada por la Oficina de las Tic, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

Por este motivo la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES como responsables de las redes de datos y los recursos de red de la institución, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Controles

- ✓ El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables con el personal de la Oficina de las Tic.

- ✓ La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y de la Oficina de las Tic.

- ✓ Todos los cambios en los servidores y equipos de red de la institución, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de Routers y Switches, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

- ✓ El acceso a Internet provisto a los usuarios de la institución es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

- ✓ La solicitud para la conexión de nuevos equipos a la red de la entidad deber hacerse a través del correo de mesa de ayuda, y desde un correo institucional, por ningún motivo se permitirá la conexión de nuevos equipos sin la previa autorización del área de sistemas.

- ✓ Solo se pueden conectar a la red los dispositivos móviles que cuenten con la aprobación del área de sistemas, para lo cual debe justificar el motivo por el cual debe conectar este a la red de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

- ✓ en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por la Oficina de las Tic.

- ✓ Los usuarios de Internet de la institución tienen que reportar todos los incidentes de seguridad informática a la Oficina de las Tic inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad de la información.

- ✓ Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que: Serán sujetos de monitoreo de las actividades que realiza en Internet, ya que Saben que existe la prohibición al acceso de páginas no autorizadas, Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados, y Saben que existe la prohibición de descarga de software sin la autorización de la Oficina de las Tic.

- ✓ La utilización de Internet es para el desempeño de su función y no para propósitos personales.

- ✓ Los servidores de red y los equipos de comunicación (Routers, switches, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

4.15 MANEJO DE CUENTAS DE USUARIOS

Política

Manejo de Cuentas de usuarios

Controles

- ✓ Toda cuenta de acceso que se requiera modificar deberá ser solicitada a la Oficina de las Tic.

- ✓ El procedimiento de creación de cuentas, debe ser canalizado a través de la mesa de ayuda.

- ✓ En caso de tener algún problema al acceder a la cuenta de usuario, el funcionario se debe notificar inmediatamente a la Oficina de las Tic y no tratar de solucionarlo.

- ✓ El área de sistemas de tener a su disposición todas las contraseñas de los equipos a cargo de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

4.16 OPERACIONES BÁSICAS DE PC

Política

Operaciones Básicas de Pc

Controles

Para el buen uso y funcionamientos de los pc deber seguirse unos pasos para asegurar su buen funcionamiento:

- ✓ Para encender el sistema de cómputo verifique que el monitor, CPU, impresora y demás periféricos estén debidamente instalados entre si y conectados a la corriente eléctrica.
- ✓ Enseguida identifique los interruptores o botones de encendido y apagado presione o mueva según se requiera.
- ✓ Encienda la Impresora, regulador, monitor, y demás periféricos que tenga instalados dejando al final el CPU.
- ✓ Para apagar el sistema presione o mueva los interruptores según se requiera en el mismo orden antes mencionado.

Cuando encender y apagar el Sistema:

- ✓ Al inicio y fin de las actividades
- ✓ En caso de tormentas eléctricas
- ✓ Si se presentan fallas eléctricas

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.17 POLITICA DE ADQUISICION Y MANTENIMIENTO DE SOFTWARE Y HARDWARE

Política: Toda adquisición de recurso tecnológico en la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, deberá contar con la revisión y aprobación previa de los requerimientos técnicos mínimos definidos, por parte del grupo de informática. La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES protegerá la propiedad intelectual propia y de terceros. El software registrado con Derechos de Autor no se podrá copiar sin previa autorización del propietario.

Todo proceso de cambio de Software deberá contar con un plan de contingencia, de tal forma que se garantice la continuidad de los procesos, la salvaguarda e integridad de la información.

Controles:

Adquisición de Equipos de Cómputo: La Oficina de las Tic verificará las características y el estado de todos los equipos digitales y análogos que ingresan a la Alcaldía de Barrancas la Guajira, previo al ingreso a almacén.

Todos los dispositivos adquiridos deben contar con la garantía de fábrica. Esta debe ser tipo ON-SITE y debe acreditarse con documento equivalente a certificación o documento expedido por la casa fabricante de cada dispositivo, la cual debe tener el tiempo de garantía, tipo de garantía y tipo de cubrimiento, además el centro autorizado para efectos de la garantía debe estar ubicado en el EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

Los equipos que hayan sido importados deben contar con el certificado de manifiesto de aduana.

La CPU y los periféricos como son monitor, mouse y teclado que adquiera la Entidad, deben ser de la misma marca. En ese sentido la entidad requiere que tanto los computadores de escritorio y equipos portátiles sean de la misma casa fabricante. Los componentes internos que conforman la CPU deberán ser respaldados por la casa fabricante de los equipos de cómputo.

Cuando los equipos de cómputo e impresoras adquiridas sean de marca de fabricación extranjera, se deberá garantizar que el respaldo de repuestos y suministros en Colombia. Mínimo para cinco (5) años (Anexar documento).

Los equipos que hayan sido importados deben contar con el certificado de manifiesto de aduana.

La CPU y los periféricos como son monitor, mouse y teclado que adquiera la Entidad, deben ser de la misma marca. En ese sentido la entidad requiere que tanto los computadores de escritorio y equipos portátiles sean de la misma casa fabricante. Los componentes internos que conforman la CPU deberán ser respaldados por la casa fabricante de los equipos de cómputo.

Cuando los equipos de cómputo e impresoras adquiridas sean de marca de fabricación extranjera, se deberá garantizar que el respaldo de repuestos y suministros en Colombia. Mínimo para cinco (5) años (Anexar documento).

Mantenimiento: Los usuarios no están autorizados para instalar o desinstalar dispositivos, o hacer mantenimiento a los equipos sin previa autorización de la Oficina de las Tic.

El Servidor Público que requiera soporte técnico debe dar aviso a la Oficina de las Tic para que allí el encargado envíe el personal especializado a diagnosticar el equipo; en caso que se presente un daño mayor el funcionario debe enviar el equipo con memorando autorizado para que ingrese al taller de mantenimiento.

Responsabilidad de la tenencia: El recurso tecnológico asignado será de uso exclusivo para labores propias de la Entidad y será responsabilidad del usuario que los retire de las instalaciones sin la respectiva autorización del jefe inmediato y registro de la novedad en la minuta de vigilancia.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Los Servidores Públicos a quienes se les asignen equipos de cómputo portátiles deberán adoptar las medidas de seguridad necesarias que garantizar la seguridad física del recurso tecnológico y salvaguardar la información.

Los servidores públicos deben dar aviso de inmediato al Almacén, de la pérdida o hurto del recurso tecnológico a su cargo, para que se surta el procedimiento establecido.

Los servidores públicos deben comunicar de manera inmediata a la Oficina de las Tic cuando detecte posibles riesgos por factores tales como humedad, inundaciones, choques eléctricos, robo, calentamientos etc.

Los usuarios no deben consumir alimentos en áreas cercanas al recurso tecnológico.

La Oficina de las Tic será la responsable de administrar las hojas de vida del recurso tecnológico, en la cual se registre todos los componentes con sus seriales, el software instalado con su número de licencia respectiva y además el registro de todos los mantenimientos realizados, tanto preventivos como correctivos.

Legalidad del Software: Todo software instalado en equipos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, será autorizado o instalado por la Oficina de las Tic, la cual tiene autonomía para desinstalar o borrar software no autorizado, en desarrollo de actividades de control de uso de software legal.

Los Servidores públicos no deben instalar en los equipos de cómputo de propiedad de la Alcaldía, Software no autorizado por la Oficina de las Tic.

El servidor público asumirá la responsabilidad por el software instalado en el computador que le sea asignado o que esté utilizando. Toda aplicación que esté instalada debe estar debidamente licenciada.

La Oficina de las Tic será la responsable del control e inventario de las licencias de software y del manejo de los medios de instalación.

Sistemas Operativos:

Aunque el sistema operativo instalado en cada equipo esté configurado para realizar las actualizaciones automáticas, los usuarios de los equipos de cómputo serán los

Responsables de mantener actualizado el sistema operativo de su equipo, teniendo la precaución de no descargar las actualizaciones de sitios no seguros.

Los equipos servidores o los que hagan sus veces, deben contar con el software para realizar el chequeo de integridad del sistema operativo y del hardware. La periodicidad de su ejecución estará definida por la persona o grupo de informática designados para ello. Esto aplica para todos los equipos de cómputo (ej.: equipos de escritorio y portátiles)

4.18 CONTRASEÑAS Y EL CONTROL DE ACCESO

Política

Controlar el acceso a la información.

Controles

- ✓ El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada, así como tampoco usar números telefónicos ni nombres de familiares. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

- ✓ Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- ✓ Cambiar la contraseña regularmente e informar del cambio a la Oficina de las Tic.

- ✓ Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.

- ✓ Nunca grabar la contraseña en una tecla de función o en un comando de caracteres pre-definido.

- ✓ Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- ✓ No utilizar la opción de almacenar contraseñas en Internet.

- ✓ Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

- ✓ Todas las contraseñas para acceso al Sistema Web con carácter administrativo deberán ser cambiadas al menos cada 8 meses.

- ✓ Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.

- ✓ Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la entidad, pudiendo ser causal de despido.

- ✓ Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

Parámetros para la creación de una contraseña:

Contraseñas fuertes que contengan números y letras, mayúsculas y minúsculas. Utilizar

contraseña que tengan por lo menos 8 caracteres alfanuméricos.

Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.

No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.

Aprobaciones Requeridas para la Creación de Usuarios y Permisos: Para la creación, actualización o bloqueo de cuentas de usuario a los sistemas de información, las solicitudes para dichas actividades deben contener de forma clara y precisa la siguiente información

1. Nombre completo del funcionario

2. Correo electrónico para notificación de contraseñas.

3. Tipo de Permiso (Consulta, ingreso de información, actualización de información, liquidación)

4. Tipo de vinculación: (Personal de planta o prestación de servicios)
5. Si es personal de prestación de servicios, la fecha final del contrato

6. En caso de solicitar acceso a más de un aplicativo se debe especificar por cada uno de ellos los permisos a los que va a tener derecho

7. Los permisos deben ser solicitados por el Director o secretario responsable de cada uno de los módulos.

Cambio forzoso de todas las contraseñas del administrador

Siempre que se detecte un ingreso no autorizado al sistema de información, los administradores del sistema deben cambiar inmediatamente cada una de sus contraseñas en el sistema.

Cambios de Contraseñas Periódicas para el Administrador

Todos los administradores deben cambiar periódicamente la contraseña en el sistema.

Control de Acceso al Sistema con Contraseña Individual para cada Usuario

Se precisa que el control de acceso al sistema, se debe realizar por medio de Usuario único, es decir que no se puede tener el acceso a la base de datos y otros recursos del sistema si no se encuentra privilegiado con uno.

La Oficina de Talento Humano reportará a la Oficina de las Tic el traslado o retiro de los servidores públicos, a fin de ejercer control sobre el estado de los usuarios.

La vigencia del usuario y contraseñas a personal de contrato estará sujeta a la fecha de finalización del contrato, siendo responsabilidad de los jefes inmediatos reportar a la Oficina de Sistemas la novedad de retiro.

Longitud de la Contraseña de Usuario

Se debe tener en la longitud de las contraseñas un mínimo de seis caracteres y una longitud máxima de cuatrocientos cincuenta y seis (456) caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Entrega de Contraseñas a Usuarios

Las contraseñas no se divulgan por medio de líneas telefónicas, se envían por correo electrónico, y el usuario debe cambiarla de manera inmediata al ingresar por primera vez a aplicativo.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Confidencialidad de las contraseñas

Se precisa que las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Hacerlo expone al usuario a responsabilizarse de acciones que otras personas hagan con su cuenta.

Los servidores públicos serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia la darán a conocer a otras personas, o harán uso de contraseñas ajenas, ni de la opción de autoguardado de contraseñas.

Cambio de contraseña cuando se sospecha que ha sido descubierta

Ante la posibilidad o sospecha de la perdida de confidencialidad de la contraseña, esta debe ser cambiada de manera inmediata y reportado el evento a la Oficina de Sistemas.

Cambio de Contraseñas Periódicas para los usuarios en el Sistema

Se precisa que todos los usuarios cambien periódicamente la contraseña en el sistema, mínimo una vez al año.

Restricción de horarios

Se implementará control de acceso a los aplicativos, en horarios autorizados por los líderes de los procesos propietarios de la información, de tal forma que si se requiere el ingreso en horario adicional al señalado, debe mediar autorización escrita del Secretario de Despacho, indicando la hora de inicio, finalización y los días que debe estar autorizado.

Bloqueo por intentos

Los intentos fallidos de acceso al sistema de información antes del límite de tres intentos, despliegan un mensaje de advertencia indicando que el usuario no ha podido iniciar sesión debido a los datos de usuario o password son incorrectos. Cuando los intentos fallidos superan el máximo de tres, se desplegará un mensaje de bloqueo de usuario, lo que implica que debe comunicarse con el administrador del sistema para el desbloqueo respectivo.

Cerrar Sesión:

Todos los usuarios deben cerrar sesión cuando no van a hacer más uso del aplicativo, o cuando van a abandonar su estación de trabajo.

Administración de usuarios.

Los Administradores de los sistemas de información, deben revisar con una periodicidad mínima mensual, los derechos de acceso de los usuarios, con el fin de actualizar el estado de los mismos ocasionado por trasladados y retiros de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

El uso de programas de acceso remoto será restringido y controlado por el área de informática, y solo podrán autorizar su utilización los líderes dueños de los procesos mediante comunicación escrita, especificando el tiempo de utilización, las actuaciones a realizar y la justificación.

Para la instalación y uso de programas de acceso remoto, el usuario autorizado debe garantizar que el acceso remoto se realizará en un equipo seguro, libre de virus, programas maliciosos y espías.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.19 CUMPLIMIENTO SEGURIDAD INFORMÁTICA

Política

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, tiene como una de sus funciones la de proponer y revisar el cumplimiento de la política de seguridad, que garanticen acciones preventivas y correctivas para el respaldo de equipos e instalaciones de cómputo, así como la de los bancos de datos de información automatizada en general.

Controles

- Los sistemas desarrollados por personal interno o externo que controle el área de Sistemas y Calidad son propiedad intelectual de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES,
- ✓ El Área de sistemas podrá implantar mecanismos de control que permitan identificar tendencias en el uso de los recursos informáticos por parte del personal interno o externo. El mal uso de los recursos informáticos que sea detectado debe ser reportado

- ✓ Esta absolutamente prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el área de sistemas.

- ✓ Ningún empleado de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, puede intentar probar fallas en la Seguridad, a menos que estas pruebas sean controladas y aprobadas por el departamento de Informática.

- ✓ Se prohíbe absolutamente la escritura, generación, compilación, copia, colección, propagación, ejecución o intento de introducir cualquier tipo de código malicioso o potencialmente dañino conocidos como virus, gusanos o caballos de Troya, diseñados con el único fin de auto replicarse para dañar o afectar el desempeño o acceso a los centros de cómputo, redes o información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

- ✓ Los jefes de área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información del DAPRE

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.20 POLÍTICA DE CONFIDENCIALIDAD DE LA INFORMACIÓN

Todos los servidores públicos que manipulen información en cumplimiento de sus funciones, y terceros tales como proveedores de redes y servicios de telecomunicaciones, personal de entes de control entre otros, deben aceptar acuerdos de uso y manejo de la información reservada o confidencial definida por la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, donde se comprometen a no revelar, modificar, dañar, eliminar o usar inapropiadamente la Información confidencial a la que tengan acceso, so pena de las investigaciones penales y disciplinarias a las que haya lugar.

Controles

- ✓ La Entidad identificará la información considerada clasificada o reservada, índice que deberá ser divulgada de conformidad con la normatividad vigente.
- ✓ La Entidad establecerá controles para el intercambio de información con terceros para asegurar la reserva e integridad de la misma y que se respeten los derechos de autor.
- ✓ La información clasificada reservada confidencial solo se debe transmitir por medios seguros.

4.21 POLITICA DE PROTECION DE DATOS Y PRIVACIDAD DE LA INFORMACION PERSONAL

Todos los funcionarios deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, redactará un “Acuerdo de Confidencialidad”, el cual deberá ser suscrito por todos los servidores públicos y contratistas. La copia firmada del compromiso debe ser retenida en forma segura por la entidad.

Mediante este instrumento, el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, esparcir o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable de la información de que se trate. A través del “Acuerdo de Confidencialidad” se deberá advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo.

Esta politica tiene como objetivo establecer las medidas generales para garantizar los niveles de seguridad y privacidad adecuados para la protección de datos personales, con

el propósito de evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados.

La presente política será aplicable a los datos personales registrados en cualquier base de datos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, cuyo titular sea una persona natural.

CONTROLES

- ✓ La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES implementará una política de Tratamiento de la información, en un lenguaje claro y sencillo, que deberá ser puesta en conocimiento de los Titulares y tendrá que incluir como mínimo:

1- Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.
2- El Tratamiento al cual serán sometidos los datos y la finalidad del mismo, si este no se ha informado por medio del aviso de privacidad.

3- Derechos que asisten a los Titulares de la información.

4- El área o persona responsable de la atención de las consultas, peticiones y reclamos ante la cual el titular de la información puede ejercer sus derechos.

5- Procedimiento por medio del cual los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar, suprimir información y revocar la autorización.

- ✓ Los mecanismos para la autorización del tratamiento de los datos personales podrán ser determinados a través de medios técnicos, de forma oral o por medio de conductas inequívocas que permitan otorgar la autorización por parte del Titular y los mismos deberán ser conservados por los responsables del tratamiento.

- ✓ Los funcionarios, contratistas o terceros sólo deberán recopilar la cantidad mínima de datos personales requerida para cumplir con los propósitos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, Dicho recaudo sólo se realizará una vez se obtenga la respectiva autorización.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- ✓ El responsable de las bases de datos deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal y así evitar su destrucción, alteración, pérdida o tratamiento no autorizado. Estas medidas deberán incluir los mecanismos de seguridad físicos y lógicos más adecuados, de acuerdo con el desarrollo tecnológico, de tal forma que garanticen la protección de la información almacenada y el secreto profesional.

- ✓ Las bases de datos que contengan datos personales, deberán ser administradas de tal modo que se garantice el respeto a derechos fundamentales como la intimidad, el buen nombre, y en especial, el *Habeas Data*.

- ✓ Ningún funcionario o contratista de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES deberá retirar o transmitir información que contenga datos personales sin la debida autorización expresa del Responsable; y en caso de que se facilite información a terceros, se deberá garantizar el buen uso y contar con el debido consentimiento para el tratamiento de los datos conforme a su finalidad, firmado por el titular de los datos. Los mecanismos de transferencia se realizarán a través de las políticas y procedimientos de seguridad y privacidad descritas en el presente manual.

- ✓ Los responsables y encargados del tratamiento de los datos personales sólo podrán recolectar, almacenar, usar o circular los datos durante el tiempo establecido para cumplir las finalidades que justificaron el tratamiento. Por lo tanto, una vez se cumpla con los objetivos y las finalidades del tratamiento, el Responsable y el Encargado deberán suprimir de una forma segura los datos personales que tengan en su posesión.

- ✓ Los funcionarios, contratistas y terceros de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, no podrán realizar el tratamiento de datos personales de niños, niñas y adolescentes, excepto cuando se trate de datos públicos. En este caso, la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, deberá respetar los intereses y los derechos fundamentales, conforme a la autorización previa del representante legal de cualquiera de ellos.

- ✓ Si no es posible poner a disposición del titular la información relacionada con las políticas de tratamiento, los responsables deberán informarle por medio de un Aviso de Privacidad sobre su existencia y la forma en la cual puede acceder a ellas, a más tardar en el momento en el que se vaya a realizar la recolección de datos personales.

- ✓ Los funcionarios, contratistas y terceros que tengan acceso a datos personales tratados y administrados por la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, deberán cumplir con la política aquí descrita, haciendo uso de los controles y medidas establecidas para la protección de la información conforme a su nivel de clasificación.

- ✓ El Responsable de las bases de datos que contengan información personal, deberá asegurar que antes de realizar cualquier tratamiento de los datos, la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, cuente con las autorizaciones de los Titulares y los mecanismos de control para la protección de la información.

- ✓ Los funcionarios, contratistas y terceros deberán evitar el acceso a los datos personales para los cuales no se encuentren autorizados yen caso de que observen violación o fallas de los mecanismos de control de seguridad y privacidad, deberán ser reportados oportunamente al Oficial de Seguridad para determinar las acciones a desarrollar.

- ✓ Toda transferencia de datos personales se deberá realizar según lo establecido en el Procedimiento Transferencia de Información de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES.

- ✓ Se deberán actualizar periódicamente las listas de acceso de las personas y funcionarios autorizados para efectuar cualquier tipo de tratamiento de datos personales. Así mismo, se identificarán, de acuerdo con los niveles de clasificación, los mecanismos apropiados para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

- ✓ Cumplido el lapso de tiempo del tratamiento de los datos personales, el Responsable deberá velar porque sean eliminados de forma segura, y evitar así su recuperación.

4.22 POLITICA DE REGISTRO Y AUDITORÍA

Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES empleará y distribuirá equipos con los controles criptográficos en toda la organización, conforme se establece en los procedimientos de seguridad de la información.

Política: Los sistemas de información que soporten los procesos críticos de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES, contarán con registros de auditoria de las actividades de usuario, de operación y administración del sistema.

Controles:

Los Log de auditoría deben proporcionar información relevante para soportar procesos de auditoría y para contribuir al cumplimiento de las políticas de seguridad de la información. Los líderes de los procesos propietarios de la información definirán los criterios a auditar de acuerdo con los requerimientos internos o externos o con los datos que considere sensibles a hechos fraudulentos.

El acceso a los logos de auditoría será restringido solo a los administradores del Sistema y a los propietarios de información o a quien estos autoricen por medios escritos.

Los administradores de los sistemas de información realizarán monitoreos trimestrales a los log de auditoría, emitiendo un acta como evidencia de la actuación y reportando las presuntas irregularidades a los líderes de los procesos propietarios de la información.

4.23 POLITICA DE DISPONIBILIDAD DEL SERVICIO

Política: La Entidad diseñará un plan de contingencia para garantizar la continuidad del servicio de los sistemas de información ante la ocurrencia de eventos inesperados.

Controles

El plan de contingencia de los sistemas de información será diseñado y evaluado semestralmente por el Jefe de la Oficina de informática y los encargados de la seguridad de los sistemas de información.

La EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES debe garantizar la disponibilidad de los recursos indicados en el plan de contingencia de los sistemas de información.

4.24 PROCEDIMIENTOS O MANEJO DE INCIDENTES ESTÁNDAR PARA TRATAMIENTO DE FALLOS

Entiéndase por Incidente todo aquel evento extraordinario que ocurra con los activos evaluados de la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES: por ejemplo, Mantenimiento preventivo de uno o todos los computadores (Anual o Preventivo), Fallo de Activos, etc. El procedimiento en cualquiera de estos casos se debe registrar teniendo en cuenta los siguientes pasos:

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

En caso de falla de un activo se debe:

1. Enviar un correo electrónico desde el correo institucional de la oficina al correo de mesa de ayuda, donde especifique:
a) nombre del usuario
b) dependencia donde labora
c) datos de contacto celular, teléfono o extensión
d) la falla que seba a reportar siendo muy claros sobre esta.

2. En caso de no poder enviar el correo debe comunicarse en su defecto al número de la mesa de ayuda para la asignación del personal y del número de caso de este.

3. En caso de no ser factible ninguna de las opciones anteriores también puede acercarse a la oficina de Mesa de ayuda donde se tomará el servicio y se asignará el técnico.

Es de vital importancia comunicar los fallos a tiempo ya que de esto depende su pronta resolución.

Para el caso de realizar mantenimiento el preventivo anual:

1. Se debe pasar el cronograma de actividades de los mantenimientos donde se especifique la dependencia sobre la cual se van a realizar, así como la fecha en que estos se van a efectuar. Lo anterior con la previa autorización del jefe o líder del área de sistemas, o el encargado del área al cual pertenezca.

2. Se deben utilizar los formatos pre establecidos para estos procedimientos.

3. En caso de algún cambio en el hardware o software del equipo, este debe ser colocado en la hoja de vida del equipo de cómputo.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.25 IMAGEN INSTITUCIONAL

- ✓ Todos los equipos podrán tener como imágenes predeterminadas aquellas que sean institucionales.
- ✓ En el exterior de todos los equipos se respetará la imagen física de empaque.
- ✓ Todos los accesorios de apoyo podrán tener plasmadas imágenes institucionales.
- ✓ Cada usuario es responsable del cuidado de su herramienta de trabajo. Por lo que se recomienda limpiar continuamente el equipo externamente.

4.26 SEGURIDAD PERSONAL

Recomendaciones Generales:

- ✓ Parpadee continuamente para evitar que las pupilas se sequen, especialmente si usa lentes de contacto.
- ✓ Cambie periódicamente la dirección de su mirada para descansar el nervio ocular.
- ✓ Realice constantemente ejercicios de visión periférica.
- ✓ Mantenga limpia la pantalla del monitor para facilitar la lectura y evitar reflejos.
- ✓ Ajuste la brillantez de la pantalla.
- ✓ Ajuste la posición de la pantalla y las fuentes de iluminación (luz natural y eléctrica).
- ✓ Coloque el monitor y los documentos fuente de manera que ambos estén aproximadamente a la misma distancia de sus ojos.
- ✓ Si utiliza lentes que sean con un marco completo para leer a una distancia de 50 a 60 centímetros.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

5. POLÍTICAS GENERALES

- ✓ Los responsables de cada área deberán apoyar al cumplimiento de los lineamientos antes mencionados.
- ✓ Todo usuario tendrá que cumplir con los lineamientos antes mencionados de lo contrario se hará acreedor a una sanción que se designará por el nivel directivo.
- ✓ Las medidas anteriores son enunciativas y no limitativas, la EMPRESA DE SERVICIOS MUNICIPALES Y REGIONALES SER REGIONALES mantendrá en contacto con los usuarios para hacerles saber de las nuevas disposiciones tecnológicas y de procedimientos.

REFERENCIAS

Ley 1450 de 2011, por el cual se expide el Plan Nacional de Desarrollo 2014-2019, en el artículo N° 55 sobre accesibilidad a servicios de TIC.

Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC– , se crea la Agencia Nacional de Espectro y se dictan otras disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital**.**

Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del Decreto 2609 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, 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, entre otras disposiciones.

Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, por la cual se dictan disposiciones generales para la protección de datos personales.