PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
2021
20 Enero de 2021

Carrera 11 No 10 – 55 Esquina Villagorgona (Candelria Valle) – Teléfono: (+57 2) 260 0979 – Celular: 3187173259
www.emcandelaria.gov.co – E-mail: contactenos@emcandelaria.gov.co – gerencia@emcandelaria.gov.co

TABLA DE CONTENIDO

1. INTRODUCCION

La Política de la seguridad de la información de EMCANDELARIA S.A.S. E.S.P asegura que la entidad establece la protección de los activos de información (funcionarios de planta, contratistas, asesores, partes interesadas, la información, los procesos, las tecnologías de información incluido el hardware y el software) dando cumplimiento a los requisitos establecidos por las partes interesadas en la gestión de la Información.

EMCANDELARIA S.A.S. E.S.P. reconoce y ha identificado la información como uno de los activos más importantes y críticos para el desarrollo eficiente de sus funciones. En la gestión de los procesos estratégicos, misionales y de apoyo, continuamente se está procesando, gestionando, almacenando, salvaguardando, transfiriendo e intercambiando información valiosa que puede ir desde un dato personal hasta documentos empresariales que no deben ser divulgados a personal no autorizado, suceso que puede poner en riesgo la gestión y administración pública de la entidad.

Por tal motivo se planteo la siguiente política: “Emcandelaria se compromete a **vigilar y verificar** el cumplimiento de la **seguridad informática** y el **tratamiento de los datos** con el fin de **preservar** la información de **los usuarios** que administra la entidad”

EMCANDELARIA S.A.S. E.S.P. cumple con los tres pilares de la seguridad de la información en preservar la integridad, confidencialidad y disponibilidad de la información (2,30 ISO 27000):

Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000)

Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)

Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000)

2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Establecer lineamientos y actividades para la implementación de políticas que garanticen la administración, manejo y control de la seguridad y privacidad de la información de EMCANDELARIA S.A.S. E.S.P., bajo la norma NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y continuidad del servicio.

3. PROCESO DE SEGURIDAD DE LA INFORMACION

EMCANDELARIA S.A.S E.S.P. con el propósito 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 usuarios tanto internos como externos.

3.1. OBJETIVOS ESPECIFICOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

- ✓ Implementar políticas y procedimientos enfocados en la de seguridad de la información.
- ✓ Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- ✓ Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, los procesos de la entidad, y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno digital con el fin de determinar la manera de implementación de los controles de seguridad requeridos para EMCANDELARIA S.A.S E.S.P

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de EMCANDELARIA S.A.S. E.S.P.

5. TERMINOS Y DEFINICIONES

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

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)

Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000)

Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).

Partes interesadas (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 tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información aceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Administración de Riesgos: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podría afectar a la información.

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

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.

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

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

Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

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

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

6. MARCO NORMATIVO

ID	NORMA	AÑO	DESCRIPCIÓN
N001	Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
N002	Decreto 1122	1999	Por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe.
N003	Decreto 1151	2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones
N004	Ley 1341	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.
N005	Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
N006	Decreto 2693	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.
N007	Ley 1712	2014	Por medio de la cual se crea la ley de Transparencia y del Derecho de Acceso a la información pública nacional y se dictan otras Disposiciones.

N008	Decreto 2573	2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
N009	Decreto 0103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
N010	Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de tecnología de la Información y las Comunicaciones.
	Decreto 1078 capítulo 1 del título 9 de la parte 2 del libro 2	2015	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital lineamientos generales de la política de Gobierno Digital
N011	Decreto 415	2016	Por el cual se adiciona el Decreto Unico Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
N012	NTC-ISO/IEC 27001	2013	Tecnología de la información, técnicas de seguridad. Sistema de gestión de Seguridad de la información
N013	NTC-ISO/IEC-27002	2013	Tecnología de la información, técnicas de seguridad. Código de practica para la gestión de seguridad de la información
N014	NTC-ISO/IEC-27005	2009	Tecnología de la información, técnicas de seguridad. Gestión del riesgo en la seguridad de la información
N015	Ley 1273 de 2009	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
N016	Ley 594 de 2000		Ley General de Archivos
N017	Decreto 2609	2012	Por medio del cual se reglamenta el Titulo 5 de la ley General de Archivo del año 2000. Incluye aspectos que se debe considerar para la adecuada gestión de los documentos electrónicos

7. RESPONSABLES

La entidad tiene como responsables de la implementación, seguimiento y mantenimiento de la Política del Plan de Seguridad y Privacidad de la información lo siguiente:

✓ El Gerente o representante legal de EMCANDELARIA S.A.S E.S.P, quien velará por el cumplimiento de la Política de Seguridad y privacidad de la Información.

✓ El representante de Control Interno quien será el delegado para velar la formulación e implementación de la Política de seguridad y privacidad de la información.

✓ Responsable de la seguridad Informática. Es el Servidor público que cumple las funciones de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los usuarios o funcionarios de la entidad que así lo requieran. Esta labor está a cargo del profesional universitario responsable del Área de informática de la entidad.

✓ Todos los funcionarios y/o contratistas y demás partes interesadas de la entidad son responsables del cumplimiento obligatorio de la Política de seguridad y Privacidad de la Información y en caso de no cumplir se reserva el derecho de tomar las medidas correspondientes según el caso.

✓ El Administrador del sistema. Es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y llevar a cabo las tareas de seguridad relativas a los sistemas que administra.

✓ Usuario. Todo servidor público o persona que asuma funciones públicas es responsable de cumplir con todas las políticas informáticas y de seguridad de la Empresa.

Para comunicar esta política se hará mediante socialización con todos los funcionarios, contratista y partes interesadas de la entidad, el cual dará a conocer la existencia, contenido y obligatoriedad de dicho documento. La custodia y ubicación física del documento estará a cargo del Sistema Integrado de Gestión y el líder de TIC.

8. POLITICAS

EMCANDELARIA S.A.S E.S.P. De acuerdo con la Política divulga 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.

CORREO ELECTRONICO: La empresa suministrará el acceso al correo electrónico y a internet, como herramientas para la realización de las labores, dependiendo de las responsabilidades y naturaleza del trabajo contratado, conforme a lo previsto en el manual de funciones. El uso inadecuado de internet constituirá una falta grave, que se clasificará como tal por la magnitud del hecho o por no atender los requerimientos de la empresa para que se cese la utilización indebida. La comprobación y las sanciones disciplinarias se realizarán conforme lo establecido en la legislación aplicable.

COMPUTADORES, SERVIDORES Y REDES: Prohibir a los usuarios la modificación de la configuración de hardware y software establecida por el funcionario encargado de administrar el sistema. Control interno será responsable que los equipos se protejan para disminuir el riesgo de hurto, destrucción, fluctuaciones de energía, incendio y medio ambiente (por ejemplo: agua), utilizando instalaciones en condiciones adecuadas, cerraduras, vigilantes, protectores contra transitorios de energía eléctrica y, para los servidores, fuentes de poder interrumpibles (UPS). Prohibir el uso de módems en computadores que tengan conexión a la red local (LAN), para prevenir la intrusión de hackers a través de las puertas traseras. Todas las comunicaciones de datos deben efectuarse a través de la red LAN de la empresa.

CUENTAS DE LOS USUARIOS: Exigir que la solicitud de una nueva cuenta o el cambio de privilegios se haga a través del funcionario encargado de la administración de la infraestructura de Red. Cuando la empresa vincula a un respectivo funcionario este debe firmar un documento donde declara conocer las políticas informáticas y de seguridad de la información y acepta las responsabilidades. No debe concederse una cuenta a personas que no sean empleados de la empresa, a menos que estén debidamente autorizados por la Gerencia o representante legal correspondiente. En este caso, la persona debe firmar un documento donde declare conocer las políticas informáticas y de seguridad de la información y acepta sus responsabilidades.

DIVULGACION DE LA INFORMACION: La información entregada a los medios de comunicación debe hacerse a través del funcionario encargado del manejo de la comunicación institucional. La empresa no se hace responsable por las consecuencias que se deriven de la utilización inadecuada por parte de terceros. Igualmente, se abstiene de suministrar la información que haya recibido de terceros para su uso interno y confidencial.

USUARIOS INVITADOS Y SERVICIOS DE ACCESO PÚBLICO:

El acceso de usuarios no registrados solo debe estar autorizado por la Alta Gerencia o representante legal a cargo, de manera de información institucional, igualmente el servicio de internet al que puedan acceder debe estar protegido con una contraseña, contando con una restricción de sitios web no autorizados. Si los usuarios invitados no realizaron el debido proceso de registro, no se permitirá el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TIC.

COPIAS DE SEGURIDAD:

Toda información que se encuentre contenida en el inventario de activos de información o que sea de interés para un proceso siempre debe estar ser respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados y probados por el Sistema Integrado de Gestión.

El procedimiento debe incluir actividades de almacenamiento, administración y custodia de las copias de seguridad incluyendo lugares seguros y control de registros de dichas copias. Dentro del procedimiento debe quedar claro que se deben efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Tener en cuenta que la creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir la responsabilidad de realizar las copias y mantenerlas actualizadas, recae directamente sobre cada dueño de los activos de la información de la Entidad.

INSTALACIÓN DE SOFTWARE

Todas las instalaciones de software que se realicen sobre sistemas operativos previamente instalados en EMCANDELARIA S.A.S E.S.P., deben ser aprobadas por la Gerencia, de acuerdo a los procedimientos establecidos para tal fin.

El funcionario encargado en la Gestión de las TIC debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad para su

respectiva investigación además debe tener un inventario del software autorizado para el uso institucional.

USO ADECUADO DE INTERNET:
La entidad es consciente de la importancia del servicio de Internet como una herramienta fundamental para el desempeño de labores que proporcionará los recursos necesarios para asegurar su disponibilidad a los servidores públicos y demás partes de interés que así lo requieran.

- ✓ El proceso de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- ✓ El proceso de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- ✓ El proceso de TIC debe monitorear continuamente el canal o canales del servicio de Internet.
- ✓ El proceso de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

SEGURIDAD EN LOS EQUIPOS: Los servidores o equipos de cómputo que contengan información institucional deben estar en un ambiente seguro y protegido por lo menos con:

- Controles de acceso y seguridad física.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Además, toda información institucional en formato digital debe ser mantenida en unidades extraíbles aprobados por la Gerencia y el líder o responsable del proceso de la TIC.
También se debe asegurar que la infraestructura esté cubierta, con mantenimiento y soporte adecuados tanto para el hardware como para el software y las estaciones de trabajo deben ser operadas por funcionarios de la institución el cual deben estar capacitados acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Se deben incluir los medios que alojan copias de seguridad el cual deben ser conservados de forma correcta de acuerdo con las políticas y estándares establecidos.

IDENTIFICACION, CONTRASEÑAS Y AUTORIZACIONES: Todos los usuarios o funcionarios que acceden a los sistemas de información requieren de un único e intransferible identificador o contraseña, el cual será proporcionado como parte del proceso de autorización. Las contraseñas concedidas deberán eliminarse o deshabilitarse, por solicitud de la Gerencia, cuando cese la vinculación del usuario o funcionario con la entidad en forma permanente o temporal, o cuando se presente un uso indebido. De esta manera, todas las acciones realizadas con una contraseña de usuario son responsabilidad del titular del mismo.