PLAN DE SEGURIDAD

Y

PRIVACIDAD DE LA INFORMACION

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

MOVILIDAD FUTURA S.A.S.

ELABORADO POR:
Profesional Subproceso de Tecnología.

Aprobado por:

ROBERTH HORMIGA

Gerente.

1. POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la entidad con respecto a la protección 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 entidad y apoyan la implementación del sistema de gestión de seguridad de la información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Movilidad Futura S.A.S, para asegurar el direccionamiento estratégico de la entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, estos correspondientes ha:

- Mitigar los riesgos de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos de la entidad.
- Garantizar la continuidad del servicio frente a incidentes.

1.1 Alcance

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la entidad y la ciudadanía en general.

1.2 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política.

A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información de la entidad.

a) La Entidad ha decidido definir, implementar, operar y mejorar de forma continua un sistema de gestión de seguridad de la información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.

b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

c) Movilidad Futura S.A.S protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.

d) Movilidad Futura S.A.S protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, 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.

e) Movilidad Futura S.A.S protege su información de las amenazas originadas por parte del personal.

f) Movilidad Futura S.A.S protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

g) Movilidad Futura S.A.S controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.

h) Movilidad Futura S.A.S implementa controles de acceso a la información, sistemas y recursos de red.

i) Movilidad Futura S.A.S garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

j) Movilidad Futura S.A.S garantiza 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.

k) Movilidad Futura S.A.S garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.

l) Movilidad Futura S.A.S garantizara el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la información, traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad.

2. IMPLEMENTACION DE POLITICAS DE SEGURIDAD DE LA INFORMACION

2.1 Justificación

Movilidad Futura S.A.S 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 perdidas, 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 coma externos.

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

a) Confidencialidad: Se garantiza que la información sea accesible solo 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:

Audibilidad: 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 solo 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.

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.

A los efectos de una correcta interpretación del presente plan, se realizan las siguientes definiciones:

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

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: Se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 Objetivo

Definir los mecanismos y todas las medidas necesarias por parte de Movilidad Futura S.A.S, tanto técnica, 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, perdida, 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

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de Movilidad Futura S.A.S, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

2.4 Roles y Responsabilidades

Es responsabilidad del Comité de Seguridad de la Información de Movilidad Futura S.A.S, 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.

2.5 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, Movilidad Futura S.A.S se reserva el derecho de tomar las medidas correspondientes.

2.6 Comunicación

Mediante socialización a todos los funcionarios de la Movilidad Futura S.A.S 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 área de MECI para que sean consultados en el momento que se Requieran, igualmente estarán alojados en la página de la entidad www. movilidadfutura.gov.co.

2.7 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 que modificaciones o adiciones deben hacerse, este monitoreo deben realizarse como mínimo una vez al año a cuando sea necesario.

3. DESCRIPCION DE LAS POLITICAS

Generalidades

Movilidad Futura S.A.S 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 para 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 entidad.

3.1 Gestión de Activos

3.1.1 Política para la identificación, clasificación y control de activos de información

Movilidad Futura S.A.S a través del comité de seguridad de la información realizara la supervisión de cada proceso, el cual debe

aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a gestión de TIC y a gestión documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El facilitador del proceso de gestión de recursos físicos con apoyo del sub proceso de tecnología tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

Pautas para tener en cuenta

a) Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

b) La información física y digital de Movilidad Futura S.A.S debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este periodo debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.

c) Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo recoger de las impresoras, escáneres, fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada a mal intencionada.

d) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que. En el momento de ausentarse de su puesto de trabajo: sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores: estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

e) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

3.2 Control de Acceso

3.2.1 Política de acceso a redes y recursos de red

El contratista de apoyo al subproceso de tecnología de Movilidad Futura S.A.S. como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso.

Pautas para tener en cuenta

a) El Subproceso de Tecnología debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.

l)) El Subproceso de Tecnología debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de Movilidad Futura S.A.S. así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las políticas de seguridad de la información por parte de estos.

c) Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de Movilidad Futura S.A.S, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de confidencialidad firmado previamente.

d) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de Movilidad Futura S.A.S deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas autorizadas.

3.2.2 Política de administración de acceso de usuarios

Movilidad Futura S.A.S establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la

entidad. Así mismo, velara porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso este regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

a) El Subproceso de Tecnología, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información de Movilidad Futura S.A.S: dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

b) El Subproceso de tecnología debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursostecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

c) El Subproceso de tecnología debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

d) Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el subproceso de tecnología, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

e) Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

3.2.3 Política de control de acceso a sistemas de información y aplicativos

Movilidad Futura S.A.S como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velaran

por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El subproceso de tecnología, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Pautas para tener en cuenta

a) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

b) Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

c) El subproceso de tecnología debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos de Movilidad Futura S.A.S.

d) El subproceso de tecnología debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

e) El subproceso de tecnología debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

f) Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

g) Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas

h) Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura. Evitando indicar específicamente cual fue la falla.

3.2.4 Políticas de seguridad física

Movilidad Futura S.A.S provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlara las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

El subproceso de tecnología mantiene las normas. Controles y registros de acceso a dichas áreas.

Pautas para tener en cuenta

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el subproceso de tecnología autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.

b) El Subproceso de Tecnología debe asegurar que las labores de mantenimiento de redes eléctricas. De voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

c) La Alta dirección debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de Movilidad Futura S.A.S.

d) La Alta dirección debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.

e) Los ingresos y egresos de personal a las instalaciones de Movilidad Futura S.A.S en horarios no laborales deben ser registrados: por consiguiente. los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

f) Los funcionarios deben portar el carnet que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de Movilidad Futura S.A.S; en caso de pérdida del carnet, deben reportarlo a la mayor brevedad posible.

g) Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

3.2.5 Política de seguridad para los equipos

Movilidad Futura S.A.S para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones. Proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Pautas para tener en cuenta

a) El subproceso de tecnología debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de Movilidad Futura S.A.S.

b) El subproceso de tecnología debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.

c) El subproceso de tecnología en conjunto con el facilitador del proceso gestión de recursos físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.

d) El subproceso de tecnología debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.

e) El subproceso de tecnología debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

f) El subproceso de tecnología debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.

g) El proceso gestión administrativa debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de Movilidad Futura S.A.S cuente con la autorización documentada y aprobada previamente por el área.

h) El proceso gestión administrativa debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad y posean las pólizas de seguro.

El subproceso de tecnología es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos: por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de Movilidad Futura S.A.S.

Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por

terceras partes deben acoger las instrucciones técnicas que proporcione el subproceso de tecnología.

k) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la Entidad, el usuario responsable debe informar al facilitador del subproceso de tecnología. con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

l) La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los profesionales universitarios de apoyo al subproceso de tecnología.

m) Los equipos de cómputo, bajo ninguna circunstancia. no deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

n) Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas. que garanticen su integridad física.

o) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

p) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

q) Los funcionarios de la entidad y el personal provisto por terceras partes asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

3.2.6 Política de uso adecuado de internet

Movilidad Futura S.A.S consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionara los recursos necesarios para asegurar su

disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad

Pautas para tener en cuenta

a) El subproceso de tecnología 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.

b) El subproceso de tecnología debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna.

c) El subproceso de tecnología debe monitorear continuamente el canal o canales del servicio de Internet.

d) El subproceso de tecnología debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

e) El subproceso de tecnología debe generar registros de la navegación y los accesos de los usuarios a internet, así coma establecer e implantar el monitoreo sobre la utilización del servicio de internet.

f) Los usuarios del servicio de internet de Movilidad Futura S.A.S deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

g) Los usuarios del servicio de internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

h) No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidos en este documento.

i) Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa,, Skype, y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de Movilidad Futura S.A.S.

j) No está permitido la descarga, uso, intercambio o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, a que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en internet debe ser autorizada por el facilitador del subproceso de tecnología o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen use del recurso.

k) No está permitido el intercambio no autorizado de información de propiedad de Movilidad Futura S.A.S, de los funcionarios, con terceros.

4. PRIVACIDAD Y CONFIDENCIALIDAD

4.1 Política de tratamiento y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales. Movilidad Futura S.A.S a través del Comité de Seguridad de la información, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales Movilidad Futura S.A.S. como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratara la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, Movilidad Futura S.A.S exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo. busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Pautas para tener en cuenta

a) Las unidades de gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir. actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

b) Las Unidades de gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

c) Las unidades de gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

d) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

e) Las Unidades de Gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

f) El comité de seguridad de la información debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de Movilidad Futura S.A.S de los cuales reciba y administre información.

g) El subproceso de tecnología debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

h) Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Los usuarios de los portales de Movilidad Futura S.A.S deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

4.2 Disponibilidad del servicio e información

Movilidad Futura S.A.S con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, a decidir crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

4.2.1 Política de continuidad, contingencia y recuperación de la información

Movilidad Futura S.A.S proporcionara los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

4.2.1.1 Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión critica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el comité de seguridad de la información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de Movilidad Futura S.A.S debe realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

El subproceso de tecnología debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad. La (el) profesional especializado con funciones de control interno debe efectuar auditorias aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

El subproceso de tecnología debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad. La (el) profesional especializado con funciones de control interno debe efectuar auditorias aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

4.3 **Transparencia y del derecho de acceso a la información publica.**

En cumplimiento a la ley 1712 de 2014 , conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública ,Movilidad Futura S.A.S facilita la disponibilidad para el acceso a la información publica y los procedimientos que tienen dercho todas las personas naturales y juridicas, para el ejercicio y la garantía del derecho fundamenta,l así como las excepciones a la publicidad de la información pública.

Por lo tanto cualquier persona puede acceder a la información pública de Movilidad Futura S.A.S de dos formas, la primera, acudiendo a la página web en donde se publica proactivamente información mínima obligatoria. La otra forma de acceder a la información es ejerciendo el derecho fundamental de acceso a la citada información mediante una solicitud dirigida a Movilidad Futura S.A.S, la cual deberá ser respondida de manera veraz y oportuna dentro del tiempo estipulado por la ley.

4.3.1 Procedimiento para el cumplimiento de la ley 1712 por parte de Movilidad Futura S.A.S

El subproceso de tecnología será el encargado de la recolección y publicación en la pagina web de la información publica con el apoyo del proceso de planeación y demás procesos involucrados, dicha información será aprobada previamente por gerencia.

1. Análisis de la información a publicar según el ITA.
2. Solicitud de la información a los diferentes lideres por medio de correo electrónico.
3. Validacion de dicha información por parte de planeación y gerencia.
4. Recoleccion de la información por parte del sub proceso de tecnología a los diferentes lideres.
5. Publicacion de la información en la pagina web.

Dicha información será actualizada cada tres meses.

Cronograma de recolección, validación y publicación de la información publica.

ACTIVIDAD	ENERO				FEBRERO				MARZO			
1												
2												
3												
4												
5												

Pautas para tener en cuenta

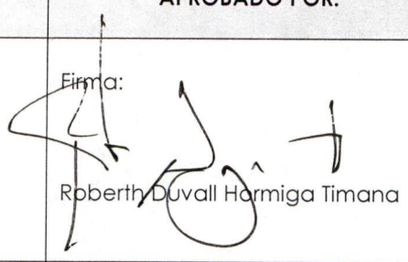
a) El Comité de Seguridad de la Información. debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

b) El comité de seguridad de la información, debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres

c) El comité de seguridad de la información debe realizar los análisis de impacto a la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

d) El comité de seguridad de la información debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información

e) El comité de seguridad de la información, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

PROYECTADO POR:	REVISADO POR:	APROBADO POR:
Firma: Amauri Montalvo.	Firma: Jairo Duque Rosero	Firma:  Roberth Duvall Hormiga Timana
Apoyo al Subproceso de Tecnología.	Líder Planeación.	Gerente

Revidado por: Contratista Monica Rodriguez- Lider Administrativa. MR