ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE MOVILIDAD	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**		
	GESTIÓN DE TICS		
	MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN		
	CÓDIGO:PA04-M01	**VERSIÓN:**004	**FECHA:** 2024-11-13

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Este documento describe las políticas específicas de seguridad de la información de la Secretaría Distrital de Movilidad. Para su elaboración, se toman como base los controles y requisitos identificados en el estándar ISO/IEC 27001 y el Modelo de Seguridad y Privacidad de la información de MINTIC.

Las políticas incluidas en este documento se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y se convierten en la base para la implantación de controles, procedimientos y estándares. La seguridad de la información es una prioridad para la Secretaría Distrital de

Movilidad y por tanto es responsabilidad de todos los funcionarios y funcionarias, contratistas y terceros velar por el continuo cumplimiento de las políticas definidas en el presente documento.

2. GLOSARIO

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. En el contexto de la norma ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”. Se puede considerar como un activo de información a:

- Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios.
- El hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información.
- Los servicios utilizados para la transmisión, recepción y control de la información.
- Las herramientas o utilidades para el desarrollo y soporte de los sistemas de información.
- Personas que manejen datos, o un conocimiento específico muy importante para la organización (Por ejemplo: secretos industriales, manejo de información crítica, know how).

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución

que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

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

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución 2352 de 2010)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (Documento Conpes 3701)

Datacenter: Centro de procesamiento de datos. Instalación empleada para albergar sistemas de información y componentes asociados donde generalmente incluyen espacio para hardware en un ambiente controlado, acondicionando el espacio con el aire acondicionado, extinción de incendios y diferentes dispositivos de seguridad para permitir que los equipos tengan el mejor nivel de rendimiento con la máxima disponibilidad del sistema.

Declaración de Aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000), implementado en la entidad con formato PA04-P01-F03 Declaración de Aplicabilidad.

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. (ISO/IEC 27000).

Información Confidencial: Información que es propia de la Secretaría Distrital de movilidad y utilizada para la ejecución de sus procesos, incluyendo bases de datos y datos sensibles (Ley 1581 de 2012), que no puede ser utilizada por terceros sin autorización previa del propietario del activo de información. En caso

de ser conocida, utilizada o modificada por personal no autorizado puede impactar de manera GRAVE a los procesos de la Secretaría Distrital de Movilidad.

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

Mecanismos de Protección de Datos Personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Partes Interesadas (Stakeholder): Persona u organización que puede afectar, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad. (ISO 9000 2015)

Plan de Continuidad del Negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de Tratamiento de Riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente. (MSPI MINTIC)

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).

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, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

SOC: Un centro de operaciones de seguridad, es un conjunto centralizado de personas, procesos y tecnología que trabajan para proteger los sistemas y redes de una organización a través de la monitorización, detección, prevención y análisis continuos de las amenazas cibernéticas.

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

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

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

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Si existen dudas sobre algún término mencionado en este documento, consulte el glosario de la Entidad en el siguiente enlace: https://www.movilidadbogota.gov.co/web/glosario.

El glosario de la Secretaría Distrital de Movilidad es una herramienta que recopila los principales términos asociados en los diferentes documentos de la Entidad, los términos se encuentran organizados alfabéticamente y las definiciones se presentan en un lenguaje claro, para una mejor apropiación por parte de los diferentes usuarios".

3. OBJETIVOS Y ALCANCE

3.1 Objetivo General

Establecer y difundir los criterios y comportamientos que deben seguir todo el funcionariado directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la Secretaría Distrital de Movilidad, o que tenga acceso a los activos de información, con el propósito de preservar la Confidencialidad, Integridad y Disponibilidad de la información, a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la Entidad, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información, de conformidad con el formato PA04-P01-F01 PLAN DE CUMPLIMIENTO DE OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN.

Para tal efecto, se obrará en concordancia con las disposiciones legales vigentes, teniendo en cuenta que estos pueden estar sujetos a modificaciones de acuerdo con su necesidad o proyección para su mejoramiento.

3.2Objetivos Específicos

- Proteger los recursos de información y tecnología frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles efectivos.

- Promover, mantener y realizar mejoramiento continuo del nivel de cultura en Seguridad de la Información, así como lograr la concientización de todo el funcionariado, contratistas y demás personas que interactúen con la Secretaría Distrital de Movilidad, para minimizar la ocurrencia de incidentes de Seguridad de la Información.
- Mantener la política de Seguridad de la Información y conjunto de políticas específicas de seguridad actualizadas, a efectos de asegurar su vigencia y eficacia.

3.3 Antecedentes

Teniendo en cuenta que el buen uso y protección de la información es un activo vital para el éxito y el cumplimiento de la misión de la Secretaría Distrital de Movilidad, este documento se encuentra alineado con la familia de normas de la serie ISO 27000 como marco de referencia para la implementación de su Sistema de Gestión de Seguridad de la Información (SGSI).

ISO 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la Seguridad de la Información utilizable por cualquier tipo de organización. Entre las distintas normas que componen la serie ISO 27000 y que fueron tomadas como referente, se resalta ISO/IEC 27001:2022 sobre los requisitos para el establecimiento del Sistema de Gestión de Seguridad de la Información.

La información, así como la plataforma tecnológica que la soporta, es considerada un activo estratégico para la Secretaría Distrital de Movilidad, por lo que es fundamental establecer políticas que definan el marco de control para brindar seguridad a los activos de información de la Entidad. Estos activos de información se constituyen en el soporte de la misión y la visión, por lo que requieren ser utilizados y manejados dentro de un adecuado entorno de seguridad, cualquiera que sea el medio y el ambiente en el que se encuentren.

La implementación del SGSI está orientada a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada el sistema efectivo que permita el tratamiento seguro de la información, además de socializar los aspectos claves del SGSI como lo contempla el formato PA04-P01-F04 Cronograma de Sensibilización del Sistema de Gestión de Seguridad de la Información.

Cuando la entidad determine la necesidad de realizar cambios al Sistema de Gestión de Seguridad de la Información - SGSI, esto se llevarán a cabo de forma planificada diligenciando en el formato Planificación de los cambios en el Sistema de Gestión de Seguridad de la Información, PA04-P01-F02.

3.4 Alcance

El presente documento define las políticas, lineamientos, controles y directrices para el Sistema de Gestión de Seguridad de la Información de la Secretaría Distrital de Movilidad.
Las políticas establecidas y sus posteriores actualizaciones aplican a todos los activos de información y las partes interesadas de la Secretaría Distrital de Movilidad.

4. MARCO DE REFERENCIA

4.1 Referencias Normativas

La normatividad específica asociada al Sistema de Gestión de Seguridad de la Información puede consultarse en la Matriz de Cumplimiento Legal de la Entidad publicada en la web en el link: https://www.movilidadbogota.gov.co/web/normatividad_aplicable

5. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1Política de Administración de Contraseñas[1]

Las y los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto, se responsabilizan de cualquier acción que se realice utilizando credenciales que le sean asignadas:

a. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
b. Las contraseñas no deberán ser reveladas.
c. Las contraseñas no se deberán escribir en ningún medio.
d. Todo el funcionariado y contratistas de la SDM, deberán realizar el cambio inmediato de la contraseña inicial entregada por los administradores de los Sistemas de Información y/o de la OTIC, con el fin de prevenir posibles ingresos no autorizados y contar con la trazabilidad y gestión de identidades de los usuarios. Esto incluye los usuarios super administradores, super usuarios y cuentas privilegiadas de administración de los sistemas de información, bases de datos, plataformas de seguridad e infraestructura tecnológica..
e. Los usuarios administradores de las cuentas con acceso privilegiado de administración de los sistemas de información, bases de datos, plataformas de seguridad e infraestructura tecnológica, deberán aceptar formalmente la responsabilidad del manejo y custodia de las cuentas asignadas mediante el uso del formato PA04-M01-F03.
f. El funcionariado y contratistas deben digitar siempre su usuario y contraseña para acceder a las diferentes aplicaciones de la Entidad; las contraseñas no se deben guardar de forma automática en los inicios de sesión de las aplicaciones; igualmente al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.
g. Toda contraseña para la cuenta de acceso debe cumplir con los estándares de contraseña segura que adopta la Secretaría Distrital de Movilidad
h. El estándar comprende las siguientes consideraciones:
    - Las contraseñas no pueden contener el nombre de la cuenta o valor del nombre del usuario. Ambos controles no distinguen entre mayúsculas y minúsculas.
    - Longitud mínima 8 caracteres.
    - La contraseña debe contener 3 de los siguientes grupos de caracteres (letras mayúsculas o minúsculas (de la A a la Z); dígitos base de 10 (0 a 9) y caracteres no alfanuméricos (caracteres especiales): (~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /) Símbolos de moneda como el euro o la libra esterlina no se cuentan como caracteres especiales para esta configuración de política.
i. Es deber de todo el funcionariado y contratistas reportar cualquier sospecha de que una persona esté utilizando credenciales de acceso o un usuario que no le pertenece, y debe catalogarse como un incidente de seguridad.
j. Los sistemas de información deben obligar el cambio de contraseña cada 45 días.

5.2 Política de Control de Acceso y Gestión de Privilegios

a. Los sistemas de información deben tener documentado el manejo de roles y privilegios de servicio.
b. El sistema de gestión de accesos e identidades de la entidad es el directorio activo.
c. Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, deben contar con una definición clara de los roles y funciones sobre estos para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.
d. La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información deberá ser revisada periódicamente por el Operador Tecnológico con el fin de mantener actualizada

dicha información y acorde con la realidad de cada una de las dependencias de la Entidad.

e. Toda persona, Sistema de Información o componente de procesamiento de información que requiera tener acceso a un componente de procesamiento de Información, contará con una cuenta única de uso exclusivo e intransferible que permite el acceso a la información de acuerdo con la necesidad de uso aprobada por el responsable de la información.
f. Cuando por funciones un funcionario, funcionaria y/o contratista requiera acceso a los sistemas de información de la Entidad, se le deberá asignar usuario y contraseña.
g. La persona responsable de la información almacenada en el componente tecnológico será el responsable de aprobar los privilegios que se asignan a la cuenta de usuario, considerando para ese fin la necesidad de acceso a información de acuerdo con las funciones que desempeñará el usuario o componente electrónico de procesamiento de información que utilizará la cuenta de acceso.
h. La asignación de toda cuenta de acceso a un componente electrónico de procesamiento de información debe cumplir con controles que permitan identificar las personas responsables de las actividades de: solicitud, aprobación, creación, modificación, inactivación o eliminación autorizada de la cuenta de acceso, así como el mantenimiento de la veracidad y trazabilidad de las actividades realizadas para la asignación de la cuenta de acceso.
i. Toda acción realizada empleando la cuenta de acceso debe ser registrada mediante controles que permitan mantener la trazabilidad de estas.
j. Toda cuenta de acceso empleará como mínimo una contraseña como mecanismo de autenticación seguro y la contraseña debe cumplir con las políticas de complejidad definidas en el presente documento.
k. Toda cuenta de acceso debe ser asignada formalmente a una persona quién responderá por su uso y acciones realizadas con la misma en el componente electrónico de procesamiento de información o con la información del componente de procesamiento de información.
l. Toda cuenta de acceso que no cuente con un responsable pasados 3 meses, debe ser inhabilitada para evitar su uso por parte de otros usuarios o componentes electrónicos de procesamiento de información que no estén formalmente autorizados y permanecerá inhabilitada hasta tanto no esté disponible el responsable de la cuenta de acceso o se decida su inactivación definitiva.
m. Para las personas contratistas naturales y/o jurídicas, las cuentas de usuario de los contratistas de la Entidad deberán contar con configuración dentro de los sistemas deinformación para que se lleve a cabo desactivación automática de acuerdo con los términos y fechas del acuerdo contractual con la SDM. Para el caso del funcionariado, es responsabilidad de la Dirección de Talento Humano llevar a cabo la notificación hacia la OTIC del funcionariado que se retire de la Entidad para que ejecute la desactivación de las cuentas de usuario.

n. En cuanto a los dispositivos que forman parte activa de la plataforma tecnológica, las personas responsables de su administración deben cambiar todas las credenciales y usuarios que traen por defecto dichos dispositivos, ya que estos son ampliamente conocidos. Una vez configurado y puesto en funcionamiento el dispositivo, se debe establecer una periodicidad para cambiar las contraseñas creadas.
o. En los sistemas de información legacy para los cuales no existe integración con directorio activo, las cuentas de usuario deben tener expiración no superior 6 meses, tiempo después del cual se deberá notificar renovación a través de la herramienta de gestión.
p. La solicitud de permisos de usuario en aplicaciones debe solicitarse a la mesa de servicios de la Entidad a través de correo electrónico mesadeservicios@movilidadbogota.gov.co o el correo electrónico que haga de sus veces, mediante el formato PA04-M01-F01 “Solicitud de cuentas de usuario”. El permiso será aprobado por la o el jefe de área del solicitante y la o el dueño (a) de la información después de ejecutada la actividad, el requerimiento será reasignado a la persona dueña de la cuenta a la que se le otorgan los permisos. La herramienta de gestión debe entregar notificación de cierre al correo del titular de la cuenta con permisos y al superior jerárquico autorizado.

q. Basado en lo anterior, la herramienta de gestión de tecnología contendrá la base dedatos de roles y privilegios otorgados y podrá ser descargada con fines de auditoría. Para la revisión de la solicitud de accesos a los sistemas de información es necesarioque la mesa de servicio lleve a cabo validación de la solicitud frente a la matriz de control de acceso por usuario PA04-M01-F04
r. Los permisos de acceso como administrador en los equipos de cómputo, es exclusivo del personal autorizado por la Oficina de Tecnologías de la Información y Comunicaciones de la Entidad y deben dar cumplimiento a las políticas de seguridad de la información de la Secretaría Distrital de Movilidad.
s. Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática de la Entidad debe estar autorizado con el respectivo control de cambios por la respectiva Oficina de Tecnologías de la Información y las Comunicaciones.
t. Todas las conexiones remotas deben ser autenticadas y seguras antes de conceder el acceso y el tráfico de datos deberá estar cifrado.
u. Todo identificador de usuario establecido para un tercero (a) o contratista debe tener una fecha de vencimiento especificada, la cual en ningún caso debe superar la fecha de sus obligaciones contractuales.
v. La asignación de privilegios en las aplicaciones para los diferentes identificadores de usuario estarán determinados por el Área dueña del sistema de información en la Secretaría Distrital de Movilidad y aprobados por la Oficina de Tecnologías de la Información y las Comunicaciones, y deben revisarse mínimo una vez al año; de igual forma se deben modificar o reasignar cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.[2]
w. Los accesos a la red inalámbrica deberán ser autorizados por la respectiva Oficina de Tecnologías de la Información y las Comunicaciones, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.

5.3 Política de Gestión de Medios Removibles[3]

a. Se encuentra restringida la conexión no autorizada a la infraestructura tecnológica de la Secretaría Distrital de Movilidad, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.
b. Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.
c. La Entidad definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones, en la plataforma tecnológica si es requerido para el cumplimiento de sus funciones.
d. Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene.
e. Para los procesos de baja, reutilización o garantías de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro.
f. El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario del activo de información.

5.4 Política de Gestión de Registros (Logs)[4]

a. Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática deberán generar registros de eventos (logs) que serán recolectados, analizados y verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información, y los dispositivos de procesamiento, de red y de seguridad de la plataforma tecnológica de la Entidad.
b. El tiempo de retención de los logs estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones vigentes.
c. Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica deberá ser reportado a la Oficina de Tecnologías de la Información y las Comunicaciones[5] y al operador tecnológico para ser solucionado a la mayor brevedad.

5.5 Política de Sensibilización, Formación y Toma de Conciencia en Seguridad de la Información[6]

a. La Secretaría Distrital de Movilidad debe mantener un programa anual de concientización y sensibilización para el funcionariado y contratistas que interactúen con la información institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.
b. Todos el funcionariado y contratistas al servicio de la Entidad deben ser informados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o ingreso cuando dichas políticas sean actualizadas y/o modificadas.
c. Todo el funcionariado, contratistas y terceros que prestan sus servicios a la Secretaría Distrital de Movilidad deben mejorar continuamente sus habilidades y competencias de acuerdo con las capacitaciones y socializaciones realizadas con relación a la seguridad de la información.
d. La Secretaría Distrital de Movilidad dispone oportunamente de los medios para desarrollar actividades que fomenten y garanticen la difusión, conocimiento, sensibilización, formación y educación del sistema de gestión de seguridad de la información.
e. Las actividades de difusión, conocimiento, sensibilización, formación y educación del Sistema de Gestión de Seguridad de la Información se realizan tomando en cuenta las responsabilidades, conocimientos y necesidades específicas de las áreas y el funcionariado a las que van dirigidas.

5.6 Política de Bloqueo de Sesión, Escritorio y Pantalla Limpia[7]

a. Cuando los sitios de trabajo se encuentren desatendidos o en horas no hábiles, las y los usuarios deben dejar bajo llave los medios que contengan información crítica protegida.
b. Las y los usuarios deben bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del usuario.
c. Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la Secretaría Distrital de Movilidad, el cual se activará automáticamente después del tiempo de inactividad definido por el responsable de Seguridad de la Información, y se podrá desbloquear únicamente con la contraseña del usuario.
d. Las y los usuarios deben retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
e. No se debe reutilizar papel que contenga información sensible.

f. Las y los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles
g. Las y los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.
h. Es responsabilidad de todos el funcionariado y contratistas borrar la información sensible escrita en los tableros o pizarras al finalizar las reuniones de trabajo y garantizar que no queden documentos o notas escritas sobre las mesas.
i. El funcionariado y contratistas, durante su ausencia del puesto de trabajo no deben conservar sobre el escritorio información propia de la entidad como documentos físicos u otros elementos, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte de terceros o personal que no tenga autorización para su uso o conocimiento.

j. Es responsabilidad de la Dirección, Subdirección, Jefe de área, Líder del Proceso o supervisor hacer diligenciar y custodiar el Acta de Responsabilidad Manejo Expedientes Físicos PA04-M01-F05, por el funcionariado o contratistas al cual se hayan asignados expedientes físicos para el desarrollo de las funciones u obligaciones según corresponda.

5.7 Política de Documentación de Procedimientos Operativos[8]

a. La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los cuales siempre deben estar a disposición de todos las y los usuarios que los necesiten para el desarrollo de sus labores.
b. Deben ser autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones, todas las solicitudes de elaboración, publicación y modificación que se realice a los documentos de seguridad de la información de conformidad con los procedimientos adoptados para tal fin.
c. Los procedimientos operativos deben contener instrucciones para el manejo de errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiere lugar.

5.8 Política de Control de Cambios Operativos[9]

a. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la Oficina de Tecnologías de la Información y las Comunicaciones y la dependencia dueña de dicho sistema; debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos tiempos e impactos potenciales asociados que puedan afectar su operación.
b. Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el Procedimiento PA04-PR04 Gestión de Cambios De TIC
c. Todos los cambios a la infraestructura de Información y Tecnología deben estar plenamente justificados.
d. Los cambios deben ser propuestos e implementados sin perjuicio de la calidad de los servicios de Información y Tecnología de Comunicaciones de la Secretaría Distrital de Movilidad.

e. Los cambios de emergencia que presenten, deben ser formalmente documentados y socializados ante el Comité de Control de Cambios de la Entidad.
f. Todos los cambios deben incluir un análisis de los riesgos de su implementación y de su no implementación.
g. Todos los cambios deben ser sometidos a algún mecanismo de prueba que permita verificar si su planificación está completa antes de su ejecución.
h. Solamente se ejecutan los cambios que han sido aprobados debidamente autorizados por el comité de Control de Cambios de la Secretaría Distrital de Movilidad.
i. Todos los cambios deben estar formalmente registrados, clasificados y documentados siguiendo los procedimientos adoptados por la Secretaría Distrital de Movilidad.
j. Todos los cambios deben contemplar acciones de marcha atrás o plan de "retirada del cambio" (rollback) en caso de un incorrecto funcionamiento tras su implementación.
k. Cuando se realicen cambios a la infraestructura de información y tecnología de comunicaciones de la Entidad se debe verificar la necesidad de actualizar los planes de contingencia y continuidad del negocio.

5.9 Política de Seguridad de la Información en la Continuidad del Negocio[10]

a. La Secretaría Distrital de Movilidad debe preservar la seguridad de la información durante las etapas de diseño, implementación y activación de las estrategias de continuidad y el retorno a la normalidad.
b. La Secretaría Distrital de Movilidad debe analizar y evaluar los riesgos relacionados con seguridad de la información y ciberseguridad para los activos de información que puedan generar una interrupción de la operación de los procesos críticos de la entidad.
c. Se deben llevar a cabo ejercicios de continuidad para mantener los planes actualizados, aumentar la confianza de la dirección en los planes y familiarizar a los colaboradores con sus responsabilidades en caso de incidentes de interrupción, contingencias o crisis.
d. La Secretaría Distrital de Movilidad debe garantizar que los sistemas de procesamiento de información críticos cuenten con redundancia suficiente para cumplir los requisitos de disponibilidad, de conformidad con lo especificado en el Sistema de Gestión de Continuidad del Negocio de la Entidad.

5.10 Política de Derechos de Propiedad Intelectual[11]

a. No se permite el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.
b. Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de estos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
c. Los procesos de adquisición de aplicaciones y paquetes de software deben cumplir con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

d. El desarrollo de software a la medida adquirido a terceras partes o realizados por funcionarios de la Entidad, deben ser de uso exclusivo de la Secretaría Distrital de Movilidad y la propiedad intelectual será de quien lo desarrolle.

5.11 Política de Sanciones Previstas por Incumplimiento[12]

a. Se sancionará administrativamente a todo aquel que viole lo dispuesto en las presentes políticas de seguridad, conforme a lo establecido por las normas que rigen al personal de la Secretaría Distrital de Movilidad y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.
b. Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga, cumpliendo las formalidades impuestas por los preceptos constitucionales, la ley de procedimientos administrativos y demás normativas específicas aplicables.
c. Además de las sanciones disciplinarias o administrativas, la persona que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial, cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el código penal y leyes especiales.

5.12 Política de Seguridad Física y Ambiental[13]

a. Las áreas seguras se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Oficina de Tecnologías de la Información y las Comunicaciones, a fin de permitir el acceso solo a personal autorizado. Estas zonas deberán estar demarcadas por un aviso que dice: SOLO PERSONAL AUTORIZADO o ZONA RESTRINGIDA.
b. Para la selección de las áreas seguras se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad de las instalaciones.
c. Las plataformas tecnológicas serán ubicadas y protegidas de tal manera que reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.
d. El cableado de energía eléctrica y comunicaciones que transportan datos o brindan apoyo a los servicios de información estarán protegidos contra intercepción o daños.
e. Se deberá garantizar la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas:

- Sistema Eléctrico suplementario
- Sistema de Control de Acceso
- Sistema de protección contra incendios

5.13 Política de Administración y Control de usuarios[14]

a. El carnet de identificación del funcionariado y contratistas es personal e intransferible y de uso obligatorio dentro de las instalaciones de la Secretaría Distrital de Movilidad.

b. Todo el funcionariado y contratistas que se encuentren dentro de las instalaciones de la Secretaría Distrital de Movilidad, están obligados a portar el carnet en forma visible para facilitar su identificación.
c. En ningún caso, el funcionariado y/o contratistas portadores del carnet, están facultados a utilizarlo en funciones diferentes o ajenas a la Secretaría Distrital de Movilidad.
d. El personal de vigilancia está en la obligación de corroborar la correcta portabilidad del carnet, al momento de ingresar a las oficinas de la Secretaría Distrital de Movilidad.
e. En caso de pérdida del carnet, el funcionariado y/o contratistas deben realizar el denuncio pertinente ante las autoridades competentes y posteriormente reportarlo a la Subdirección Administrativa de la Secretaría Distrital de Movilidad.
f. Cuando un funcionario (a) se desvincule laboralmente de la Secretaría Distrital de Movilidad, deberá entregar el carnet de acuerdo a lo dispuesto en el formato PA02-IN08-F01" listado de documentos para la entrega del puesto de trabajo". De igual manera, para la terminación de un contrato por prestación de servicios, la persona contratista deberá entregar el carnet de acuerdo a lo dispuesto en el formato PA05-M03-F09.
g. Todas las puertas que utilicen sistema de control de acceso deberán permanecer cerradas, y es responsabilidad de todo el funcionariado y contratistas evitar que las puertas se dejen abiertas. Las personas que tengan acceso al Datacenter serán definidas única y exclusivamente por la Oficina de Tecnologías de la Información y las Comunicaciones.
h. Las y los visitantes se deben registrar en la recepción y deberán ser autorizados y permanecer acompañados de un funcionario (a) cuando se encuentren dentro de las instalaciones de la Entidad. La identificación suministrada por la empresa de seguridad debe mantenerse en un lugar visible durante su estancia en las instalaciones.
i. Es responsabilidad de todo el funcionariado y contratistas acatar las normas de seguridad y mecanismos de control de acceso de la Entidad, dispuestos por la empresa de seguridad privada contratada para tal fin.

5.14 Política de Trabajo en Áreas Seguras[15]

Dentro de las políticas de trabajo en áreas seguras se encuentran las siguientes:

- Centro de datos.
- Centros de cableado.
- Áreas de tesorería.
- Archivo, áreas de recepción y entrega de correspondencia.
- Centro de Gestión de Tránsito

Estas áreas seguras deberán contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información de la Secretaría Distrital de Movilidad.

a. En las áreas donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:
    - No se debe ingresar sin la correspondiente autorización. Toda persona que esté autorizada para ingresar a las áreas seguras debe registrar sus datos en la planilla definida para ello, al ingresar y abandonar el área.
    - No se deben consumir alimentos ni bebidas.
    - No se deben ingresar elementos inflamables.
    - No se debe permitir el acceso de personal ajeno sin que esté acompañado por un funcionario durante el tiempo que dure su visita.

- No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
- No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
- No se permite el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

b. Las áreas seguras deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos y el estado de los medios que contienen información, así como un sistema de detección y control de incendios. Debe existir un extintor tipo C[16], verificando las especificaciones de seguridad contra incendios de medios eléctricos y electrónicos.

c. El Data Center debe contar con un sistema de control de acceso biométrico (huella dactilar), tarjeta de proximidad y clave para el ingreso de personal autorizado.

5.15 Política de Supervisión de la Seguridad Fisica

La Subdirección Administrativa deberá:

a. Instalar circuito cerrado de televisión (CCTV) para la vigilancia de los equipos y usuarios internos o visitantes que realicen funciones con activos de información de alta criticidad.

b. Implementar avisos de privacidad conforme a las obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios.

c. Monitorear periódicamente las actividades de los usuarios internos y visitantes en las instalaciones de la Secretaría Distrital de Movilidad a través de un circuito cerrado de televisión y/o marcación de puntos en las rondas de vigilancia.

5.16 Política de Ubicación y Mantenimiento de los Equipos[17] [18]

a. Los equipos que hacen parte de la infraestructura tecnológica de la Secretaría Distrital de Movilidad deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado a los mismos.

b. La Entidad adoptará los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.

c. El funcionariado y contratistas velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.

d. Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichos equipos no se vean afectadas por obsolescencia. Por lo tanto, la Entidad revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.

e. Los equipos portátiles deberán estar asegurados con un mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de la Entidad.

f. La Secretaría Distrital de Movilidad garantizará la existencia de pólizas o seguros para la reposición de los activos informáticos que respaldan los planes de contingencia y la

continuidad de los servicios.

g. Los equipos de contratistas y demás terceros que hayan sido autorizados para acceder de forma permanente a la red de la Entidad deben permanecer dentro de las respectivas instalaciones hasta la finalización del contrato o las labores para las cuales estaba definido.

5.17 Política de Seguridad de los Equipos Fuera de las Instalaciones[19]

a. El uso de cualquier equipo de almacenamiento y procesamiento de información por fuera de las instalaciones de la Entidad deberá ser aprobado por el jefe del área y la Oficina de Tecnologías de la Información y Comunicaciones.
b. Las y los usuarios que requieran usar los equipos fuera de las instalaciones de la Secretaría Distrital de Movilidad deben velar por la protección de estos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometida la imagen o información del sector.
c. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información clasificada o reservada, se deberá realizar inmediatamente el respectivo reporte y se deberá poner la denuncia ante la autoridad competente, si aplica.[20]
d. Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de la Secretaría Distrital de Movilidad deben contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene.

5.18 Política de Intercambio y Transferencia de Información

a. La información propiedad de la Secretaría Distrital de Movilidad o que se encuentra bajo su custodia, se debe controlar siguiendo las políticas de seguridad de la información de la Entidad y la reglamentación a la cual está sometida la Entidad.
b. El intercambio de información con terceros debe ser aprobado formalmente por los dueños de la información, mediante debido acuerdo, convenio o contrato según corresponda
c. La Secretaría Distrital de Movilidad para la regulación del intercambio de información entre Entidades para el cumplimiento de funciones públicas tendrá en cuenta lo establecido en el Decreto Nacional 2280 de 2010 del Ministerio De Hacienda y Crédito Público por el Por el cual se modifica el artículo 3o del Decreto 235 de 2010 el cual establece: “Artículo 3o. Para efectos de formalizar el intercambio de información, de manera ágil, oportuna y confiable, las entidades públicas o los particulares encargados de una función administrativa podrán emplear el mecanismo que consideren idóneo para el efecto, tales como cronograma de entrega, plan de trabajo, protocolo o convenio, entre otros”
d. Para el intercambio de información se deben establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir o suministrar la información que por mandato legal se requiere, o permitir el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras Entidades para el ejercicio de sus funciones.
e. La Secretaría Distrital de Movilidad debe proveer los mecanismos e implementar los controles necesarios para asegurar que no se presenten fugas de información a través de canales no autorizados.
f. Cuando se apruebe el intercambio de información con un tercero, se deberá suscribir previamente contratos y acuerdos de confidencialidad de acuerdo con el formato establecido

PA04-M01-F02 “Acuerdo de confidencialidad” en los cuales se señalarán los términos y condiciones para la entrega de la información requerida.

g. Cuando se intercambie información clasificada como confidencial, se debe cifrar siguiendo la política y controles definidos por la Secretaría Distrital de Movilidad para la protección de dichos tipos de información.

h. La entrega de información no concede autorización expresa o implícita, o permiso o licencia de uso de marcas comerciales, patentes, derechos de autor o de cualquier otro derecho de propiedad industrial o intelectual sobre la información que sea suministrada por la Secretaría de Movilidad a un tercero.

i. Para el cumplimiento de la política de intercambio de Información, las áreas responsables de la información deben coordinar sus esfuerzos con el Comité Institucional de Gestión y Desempeño vigente de la Secretaría Distrital de Movilidad (o quien haga sus veces) para la lograr implementación de los controles que se identifiquen como necesarios para el intercambio de información.

j. El funcionariado y contratistas de la Entidad que en el desarrollo de sus tareas habituales u ocasionales deban realizar actividades relacionadas con el intercambio de información dentro de la Entidad o con terceros, son responsables del cumplimiento y seguimiento de esta política.

k. La información de la Entidad debe ser empleada para servir a una finalidad operativa y administrativa en relación con la Secretaría Distrital de Movilidad. Cualquier Información de la Entidad es susceptible de ser auditada para propósitos de control interno, control de calidad o investigación de incidentes de seguridad de la información, en consecuencia, la o el usuario (a) reconoce y acepta que la información institucional que sea objeto de intercambio puede ser analizada siguiendo los procedimientos administrativos a los que está sujeta la Entidad.

l. Las y los terceros que reciban información de la Secretaría Distrital de Movilidad se deben comprometer a proteger toda información que les sea suministrada por parte de la Secretaría Distrital de Movilidad, sin importar su nivel de clasificación para evitar su divulgación no autorizada aplicando los procedimientos administrativos, técnicos o legales que se acuerden con la Secretaría Distrital de Movilidad al momento de recibir la información.

5.19 Derechos de Propiedad Intelectual de la Secretaría Distrital de Movilidad

a. Los documentos, datos, estudios técnicos, la cartografía y toda la información que puedan contener los medios análogos, los soportes físicos y los archivos entregados por la Secretaría Distrital de Movilidad, son propiedad de la Entidad y en consecuencia se encuentran protegidos por las leyes de propiedad intelectual vigentes en Colombia, así como por los convenios y tratados internacionales aplicables a la materia. En la medida de lo anterior la o el receptor (a) de la información se obliga a no exportar o reproducir los archivos o datos relacionados a ningún otro sitio diferente al que se especifique con la Entidad al momento del recibo de la información.

b. Al momento de la entrega de la información, la Secretaría Distrital de Movilidad definirá la limitación de derechos para el uso de la información. La Secretaría Distrital de Movilidad mantendrá en todos los casos los derechos de autor de la información generada por la Entidad.

c. La información, datos o documentos entregados por la Secretaría Distrital de Movilidad a TERCERAS PARTES no se podrá comercializar, ni prestar, ni copiar, ni compartir, ni reproducir, ni arrendar, ni enajenar, ni prestar servicios a TERCEROS no autorizados expresamente por la Secretaría Distrital de Movilidad y sólo podrá ser copiada, compartida, reproducida o utilizada exclusivamente para realizar las actividades que sean expresamente autorizadas por la Secretaría Distrital de Movilidad al momento de la entrega de la información.

d. Los documentos o información suministrada por la Secretaría Distrital de Movilidad se utilizarán exclusivamente para las actividades propias del acuerdo que se establezca con el TERCERO. En el caso que objeto genere algún tipo de documento o publicación estos deberán contener la

siguiente atribución de derechos de propiedad de la Secretaría Distrital de Movilidad *"Este documento incluye información de propiedad de la Secretaría Distrital de Movilidad y se utiliza bajo su autorización, todos los derechos sobre la información propiedad de la Secretaría Distrital de Movilidad están reservados a la Entidad"*.

5.20 Política de Seguridad de la Información en la Gestión de Proyectos

La política aplica a todo el funcionariado, contratistas y terceros, entre otros que tengan una relación directa con la Secretaría Distrital de Movilidad con el fin de preservar la seguridad de la información en la entidad y mitigar posibles vulnerabilidades de seguridad que puedan ser generadas durante las etapas de los proyectos que lleven a cabo dentro de la Secretaría Distrital de Movilidad y que requieran tratamiento de la información.

Por lo anterior, es necesario dar cumplimiento a los siguientes lineamientos:

a. Se debe integrar la seguridad de la información en la gestión de cada uno de los proyectos que tienen como fin apoyar los procesos misionales dentro de la Secretaría Distrital de Movilidad independientemente de su naturaleza, con el fin de asegurar que los riesgos asociados a seguridad de la información sean identificados y se traten dentro del proyecto.
b. Las y los responsables de la gestión de proyectos dentro de la Secretaría Distrital de Movilidad, deben valorar y validar que los objetivos del proyecto no se encuentren en contravía con las políticas de seguridad de la información de la Entidad.
c. Los riesgos de seguridad de la información deben ser identificados dentro de las primeras etapas de la Gestión de Proyectos de la Secretaría Distrital de Movilidad y se debe realizar un seguimiento de estos para identificar controles adicionales necesarios para salvaguardar la información de la Entidad.
d. Las y los supervisores de los contratos o responsables de los proyectos deben reportar los eventos o riesgos de seguridad a través del mecanismo asignado para las notificaciones de incidentes de seguridad de la información teniendo en cuenta la Guía de Gestión de Incidentes de Seguridad de la Información PA04-G01 .
e. Cualquier incumplimiento de los requisitos de seguridad de la información establecidos para los proyectos deben ser informados oportunamente por la persona supervisor (a) del contrato o responsable del Proyecto a las partes interesadas incluyendo la Oficina de Tecnologías de la Información y Comunicaciones de la Secretaría Distrital de Movilidad para tomar las acciones necesarias
f. Los requisitos de seguridad de la información en todos los proyectos deben ser definidos por las y los responsables de los mismos, los cuales deben ser aceptados e implementados durante todo el ciclo de vida del proyecto y se deberán realizar revisiones periódicas de acuerdo a la complejidad del proyecto y en caso que la persona supervisor (a) lo requieran.

5.21 Política de Relación con Proveedores

5.21.1 Planificación de las Relaciones con Proveedores y Cadena de Suministro TI

a. Identificar y evaluar los riesgos de seguridad de la información que acompañan la posible adquisición del producto o servicio. Si se considera pertinente, llevar a cabo la gestión de riesgos de acuerdo con la metodología establecida dentro de la Guía PE01-G01 Guía metodológica para la gestión de riesgos.
    - Deberá ser proporcional a la criticidad del producto o servicio que se planea adquirir, incluyendo de ser necesario la cadena de suministro de tecnologías de la

información desde el momento de la planeación hasta el momento de entrega del producto o servicio.
- Tener en cuenta los requisitos legales y regulatorios aplicables al producto o servicio que se planea adquirir para garantizar que se hayan obtenido los permisos y licencias formales antes de iniciar la relación con el proveedor.

b. Identificar el nivel aceptable de riesgos en la relación con el potencial proveedor.
c. Identificar y evaluar opciones para el tratamiento de los riesgos identificados y evaluados.
d. Definir e implementar un plan de tratamiento de riesgos de seguridad de la información para que los riesgos identificados y evaluados sean mitigados al nivel de riesgo aceptable.
e. Definir un plan de relación con proveedores del producto o servicio que se prevé adquirir. En particular, el plan de relación con proveedores deberá contener lo siguiente:
   - Especificaciones del producto o servicio que se prevé contratar, en particular su alcance, audiencia, tipo y naturaleza.
   - Activos, tales como servidores, bases de datos, aplicaciones, infraestructura de red, que tengan relevancia para la seguridad de la información en el uso del producto o servicio, y sus propietarios asociados.
   - Entradas de clasificación de información de la Entidad, la clasificación de información del proveedor y otros controles de seguridad de la información.
   - Los requisitos legales y regulatorios aplicables a la Entidad, y las áreas de leyes y reglamentos que vinculan al proveedor potencial que deben revisarse durante el proceso de selección de proveedores, según aplique.
   - Roles y responsabilidades de seguridad de la información asignados dentro de la Entidad y específicos del producto o servicio que se puede adquirir.
   - Información de la Entidad que se puede compartir con posibles proveedores del producto o servicio.
   - Requisitos mínimos de seguridad de la información que se acordarán con el proveedor seleccionado para la adquisición del producto o servicio. Estos requisitos deben resultar directamente del plan de evaluación y tratamiento de riesgos de seguridad de la información y del marco de requisitos de seguridad de la información definido en la estrategia de relación con el proveedor.
f. Realizar un proceso de articulación del entorno de red que contemple los elementos físicos, virtuales y en la nube y la interacción entre ellos, según aplique.

5.21.2 Selección de Proveedores

Definir e implementar criterios de selección de proveedores que contenga especificaciones del producto o servicio que se puede contratar y en el marco de criterios de selección de proveedores definidos. Los criterios de selección de proveedores cubrirán lo siguiente:

a. Aceptación por parte del proveedor de los requisitos de seguridad de la información definidos en el pliego de condiciones.
b. Madurez del proveedor en seguridad de la información, cuando se considere necesario.
c. Los términos bajo los cuales el proveedor permite ser auditado por la Entidad o por un tercero autorizado para verificar el cumplimiento de los requisitos de seguridad de la información definidos.
d. Aceptación transitoria cuando el producto o servicio a contratar haya sido previamente explotado o fabricado por la Entidad o por otro proveedor.
e. Aceptación de terminación para mantener la seguridad de la información en caso de terminación del contrato de relación con el proveedor.
f. Gestión de la capacidad del proveedor para suministrar el producto o servicio que pueda contratar,

g. Fortaleza financiera del proveedor que puede suministrar el producto o servicio. y la ubicación del proveedor y desde donde se suministrará el producto o servicio. Se debe tener especial cuidado para identificar esta ubicación con el fin de:
    - Identificar cualquier riesgo legal y regulatorio potencial causado por la diferencia en las leyes y regulaciones entre la Entidad y el proveedor.
    - Garantizar que las obligaciones legales y reglamentarias que se aplican al proveedor no puede afectar negativamente el acuerdo de relación con el proveedor en términos de seguridad de la información

h. Preparar un acuerdo de confidencialidad de acuerdo con el formato PA04-M01-F02 “Acuerdo de confidencialidad con la SDM” para ser firmado por el proveedor para proteger los activos de la Entidad, como información y sistemas de información transmitidos durante el proceso de selección de proveedores. Este acuerdo de confidencialidad debe ser firmado por el proveedor potencial antes de cualquier intercambio de información que se relacione con el producto o servicio que se pueda contratar.

i. Preparar y proporcionar un documento de licitación al proveedor potencial. El documento debe contener información suficiente para que el proveedor pueda preparar su propuesta con fundamento. En particular, el pliego de condiciones deberá contener lo siguiente:
    - Especificaciones (p. ej., alcance, audiencia, tipo y naturaleza) del producto o servicio a adquirir.
    - Requisitos de seguridad de la información que el proveedor deberá seguir mientras suministre el producto o servicio.
    - Niveles de servicio o indicadores clave de desempeño a seguir durante el suministro del producto o servicio.
    - Las posibles sanciones que puede imponer la Entidad en caso de incumplimiento de los requisitos de seguridad de la información considerando las siguientes condiciones:
        - En la medida de lo posible, el pliego de condiciones solo debe contener contenido público o desclasificado. Dicho documento solo debe contener la información necesaria para permitir que el proveedor responda justificadamente.
        - La información altamente sensible nunca debe incluirse en un documento de licitación en ninguna circunstancia.
        - Se deben recopilar los documentos de respuesta que han sido transmitidos por proveedores potenciales en respuesta al documento de licitación y estos deben ser evaluados con base a los criterios de selección de proveedores.
    - Seleccionar un proveedor basado en la evaluación de estos documentos de respuesta.

5.21.3 Negociación de Acuerdos con Proveedores

a. Asegurarse de que la otra parte haya recibido el documento de relación con el proveedor y de que comprenda completamente los aspectos de seguridad de la información contenidos en el mismo.

b. Operar la transición del producto o servicio de acuerdo con el plan de transición acordado y notificar a la otra parte de manera oportuna en caso de que ocurran eventos inesperados durante esta actividad.

c. Gestionar los eventos e incidentes de seguridad de la información de acuerdo con los procedimientos acordados.

d. Capacitar periódicamente al personal que pueda estar involucrado en la ejecución del plan de terminación.

e. Gestionar otros cambios, que puedan impactar en el suministro del producto o servicio contratado, cuando sean notificados por la otra parte:
   - Cambio en el negocio, la misión o el entorno.
   - Cambio relacionado con la solidez financiera.
   - Cambio de propiedad, o creación de uniones temporales.
   - Cambio de ubicación desde donde se adquiere o suministra el producto o servicio.
   - Cambio en el nivel de seguridad e implementación de controles en la organización.
   - Cambio en las capacidades requeridas de continuidad del negocio.
   - Cambio en los requisitos legales, regulatorios y contractuales aplicables.

f. Asegurarse de que las actividades de monitoreo y supervisión cumplan con el plan asociado y el proceso de manejo de acciones correctivas. En caso de que ocurran cambios en los riesgos de seguridad de la información o de no conformidades de auditoría, la Entidad con el apoyo del proveedor deberá:
   - Identificar y evaluar los impactos en la seguridad de la información resultantes de estos cambios o auditar las no conformidades.
   - Determinar si se deben reconsiderar los aspectos de seguridad de la información definidos en el contrato con el proveedor.
   - Determinar qué acciones correctivas se deben implementar dentro de una escala de tiempo definida y acordada para recuperar un nivel aceptable de seguridad de la información dentro del alcance del producto o servicio adquirido.

g. Acordar con el proveedor:
   - Los cambios por realizar en los aspectos de seguridad de la información definidos en el contrato con el proveedor.
   - Medidas correctivas aplicables
   - Aprobar el contrato con el proveedor.

5.21.4 Gestión de Relaciones con Proveedores

a. Establecer las actividades que deben ser tenidas en cuenta por la Entidad, para la gestión de la prestación de los servicios o productos contratados, verificación de las responsabilidades y controles aplicables para dar alcance al objeto contractual, por lo cual se recomienda:
   - Asegurar que los documentos y pólizas se encuentren vigentes durante el periodo de ejecución, en caso de prorrogas estar atentos a las actualizaciones contractuales que den a lugar.
   - Realizar revisiones periódicas a los documentos, planes y procedimientos entregados por el proveedor, sobre los cuales basan la operación, para determinar la funcionalidad y/o necesidad de actualización o mejoras que permita ajustarse al proceso y políticas existentes de la Entidad.
   - Evaluación de riesgos de seguridad de la información de forma periódica en acuerdo con el con el proveedor, para determinar posibles nuevas amenazas o vulnerabilidades en los productos o servicios contratados, los cuales como resultado deberán ser gestionados por el proveedor del servicio de acuerdo con los Acuerdos de Nivel de Servicio establecidos en el contrato.
   - Adoptar los procedimientos del proveedor según corresponda, a los procesos existentes en la Entidad, para así alinear las estrategias de continuidad del negocio entre las partes, de acuerdo al Sistema de Gestión de Continuidad del Negocio.

- Verificar la ejecución del plan de capacitación y realizar las mediciones sobre la efectividad y nivel de apropiación de los conocimientos de los asistentes.
- Contar con un plan de gestión de cambios que permita tener control y trazabilidad de las acciones realizadas por el proveedor.
- Establecer un plan terminación que incluya entre documentación para la transición, métodos de intercambio de datos, reglas o registros (si aplica), que permita un proceso transparente en el caso que no sea posible o adecuada la continuidad con el proveedor.
- Contar con un repositorio único en el cual se cuente con la información de la ejecución contractual tales como registros, documentos, procedimientos, manuales, listados y en general todos aquellos que sean considerados como elementos de valor o evidencias durante la ejecución contractual.
- Realizar un monitoreo de las actividades y acciones de los servicios en la nube.

5.21.5 Proceso de Terminación de la Relación con el Proveedor

a. Establecer las actividades a realizar para la finalización contractual con el proveedor de productos o servicios de seguridad de la información, para ello, es importante establecer y contar con un plan de terminación que contemple diversas actividades con el objetivo de mantener la continuidad en la operación para ello es necesario:
   - Describir las actividades y procedimientos generales para tener en cuenta durante el cierre y posterior a la finalización del servicio sin que se incurran en costos adicionales para las partes.
   - Coordinar las actividades de cierre de los servicios contratados acorde al plan de finalización.
   - Durante el proceso de entrega, el proveedor deberá relacionar documentación técnica, bitácoras de procedimientos, registros actualizados, y en general toda la información que sea parte integral y de relevancia sobre las labores adelantadas durante la ejecución contractual.

b. De acuerdo con el servicio deberán ser requeridos en la entrega como mínimo:
   - Documentación técnica del diseño y de la operación.
   - Archivos de Imágenes de máquinas virtuales.
   - Archivos de bases de datos.
   - Archivos de bases de datos de administración de configuraciones (CMDB).
   - Archivos que se encuentren dispuestos en los servicios de almacenamiento contratado.
   - Toda aquella documentación sobre topologías o estructuras físicas o lógicas.
   - Solicitar apoyo al proveedor o al comité técnico durante el proceso de cierre contractual para la coordinación de los despliegues técnicos, y operativos que sean necesarios para verificar, probar, trasladar y ejecutar la entrega o migración de los productos o servicios de seguridad de la información.
   - Solicitar certificación al proveedor la cual indicará la eliminación total y segura de los datos almacenados con herramientas especializadas que no permitan la recuperación o reuso.
   - Acta de finalización del proceso contractual avalada y firmada por el supervisor, en el cual certifica el cierre del proceso contractual.

- Verificar el cambio de credenciales de acceso, eliminación de usuarios y cierre de conexiones remotas al proveedor saliente.

5.22 Política de Acuerdos de Confidencialidad [21]

Todo el funcionariado, contratistas y demás terceros deben firmar el acuerdo de confidencialidad de acuerdo con el formato **PA04-M01-F02** “Acuerdo de confidencialidad de la SDM” y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

5.23 Política de Seguridad de la Información para la Relación con Contratistas

a. En todos los contratos cuyo objeto sea la prestación de servicios a título personal, bajo cualquier modalidad jurídica, que deban desarrollarse dentro de las instalaciones de la Secretaría Distrital de Movilidad, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar.
b. En ningún caso se otorgará 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 definan las condiciones para la conexión o el acceso.
c. El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica de la Entidad debe ser solicitado por la persona supervisor (a), o persona a cargo del tercero, al propietario de dicho activo. Este, junto con la Oficina de Tecnologías de la Información y Comunicaciones o la que haga sus veces, aprobará y autorizará el acceso y uso de la información.
d. Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, deberán contemplar como mínimo los siguientes aspectos:
    - Forma en los que se cumplirán los requisitos legales aplicables
    - Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
    - Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos
    - Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible
    - Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
    - Niveles de seguridad física que se asignará al equipamiento tercerizado.
    - Derecho a la auditoría por parte de la Secretaría Distrital de Movilidad.

5.24 Política de Uso de Dispositivos Móviles

a. Se debe separar la información privada de la institucional cuando dicha información esté contenida en un mismo dispositivo móvil.
b. Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se deben implementar controles de acceso y mecanismos

de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la Seguridad de la Información.

c. La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser autorizada por la Oficina de Tecnologías de la Información y las Comunicaciones, previa verificación de que cuenten con las condiciones de seguridad y estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.

d. El Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Movilidad vigente de la Entidad (o quien haga sus veces) de acuerdo con la tecnología existente definirá las directrices necesarias para la aprobación de conexión de equipos de tecnología móviles tales como celulares, portátiles, tabletas y teléfonos inteligentes entre otros, a las redes de la Secretaría de la Movilidad.

e. La Entidad deberá adoptar mecanismos que permitan identificar los equipos pertenecientes a terceros, así como los mecanismos de control de seguridad de la información que se debe cumplir para tener acceso a la infraestructura tecnológica de la Secretaría Distrital de Movilidad.

5.25 Teletrabajo y Trabajo en Casa[22]

a. El Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Movilidadde acuerdo con las necesidades misionales, definirá las directrices necesarias para la aprobación de actividades de teletrabajo y trabajo en casa de acuerdo con las necesidades de la Entidad, características de trabajo dentro o fuera de la Entidad,modalidades (trabajadores con contrato laboral, trabajadores independientes,trabajadores que utilizan dispositivos móviles), beneficios y obstáculos de acuerdo a laley 1221 de 2008, al decreto 0884 de 2012, artículo 2° del Decreto Distrital 806 de 2019 o a la normatividad vigente, los requerimientos del Sistema de Gestión de Seguridad de la información - SGSI de la Entidad y los resultados de los análisis de riesgos. En cualquiera de los dos tipos de trabajos mencionadas, el personal autorizado para ejercer sus labores y/o responsabilidades funcionales, debe cumplir las siguientes acciones y condiciones:

- El funcionariado o contratista acordará con la Secretaría Distrital de Movilidad los equipos de cómputo o dispositivos a utilizar para conectarse a la infraestructura tecnológica de la Entidad para realización de las labores funcionales o contractuales en el sitio del teletrabajo o trabajo en casa en Colombia o fuera del país, según la modalidad de contratación. En cualquiera de los equipos de cómputo que se acuerde entre las partes, el funcionariado o contratistas deben realizar acciones que establezcan la seguridad física de dichos equipos en la residencia o lugar donde ejercerán sus funciones y obligaciones, según corresponda. En tal caso se deberán contemplar las siguientes recomendaciones establecidas:

  Secretaría Distrital de Movilidad:

  - Implementar en la Entidad canales de comunicación seguros desde Internet como SSL[23] VPN[24], para todo el funcionariado y contratistas en las conexiones para teletrabajo y trabajo en casa.
  - Implementar soluciones de almacenamiento como Drive corporativo para guardar los archivos de las y los colaboradores a través de la infraestructura del servidor de archivos implementada.
  - Activar perfiles de navegación para los usuarios SSL/VPN permitidos. Realizar monitoreos permanentes a la infraestructura de los servicios utilizados por los teletrabajadores, con el fin de analizar posibles acciones no autorizadas.
  - Implementar validaciones de seguridad mínimas al momento de la conexión por SSL VPN, para dispositivos BYOD (Bring Your Own Device), como protección de antivirus, actualización de parches de seguridad entre otros.
  - Impedir guardar de forma automática las credenciales de usuarios asociadas a las herramientas corporativas. Generar políticas de backup para evitar pérdidas de información.

- Implementar políticas de cifrado en los equipos, servidores y herramientas transaccionales con el fin de mantener la protección de la información. Implementar la segmentación (mínimo privilegio) en los recursos a los que se accederá de forma remota con el fin de garantizar que ante un acceso indebido al equipo que se está intentando conectar a la red, no pueda acceder a recursos y/o información que no es necesaria para ese usuario.
- Hacer uso de herramientas de protección del dispositivo como EDR (Endpoint Detection and Response), los cuales permiten una gestión integral y centralizada de la política de seguridad de la Entidad localmente en los dispositivos del funcionariado.
- Se debe asegurar que en caso de extravío de dispositivos se deben configurar medidas de seguridad para proteger la información corporativa (localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas).

Funcionariado y Contratistas

- Cambiar las claves el acceso a wifi y evite utilizar redes inalámbricas abiertas, puede presentarse pérdidas de información.
- Realizar copias de seguridad de manera periódica haciendo uso de los medios de almacenamiento entregados por Entidad para tal fin.
- No enviar archivos con información de la Entidad, por medios no oficiales como whatsapp, dropbox, wetransfer, correos de dominio gratuito, etc.
- Cerrar la sesión cuando no se esté usando el dispositivo, tanto en casa como en lugares públicos.
- Mantener actualizado el sistema operativo con los últimos parches de seguridad liberados por el fabricante, si trabaja desde su propio dispositivo.
- Instalar y mantener actualizado el software antivirus, de un fabricante reconocido, para evitar infecciones con virus o software malicioso.
- Tener un espacio adecuado para teletrabajar sin riesgo a perder información por causa de daño del equipo por la mala manipulación de alimentos, por ejemplo.
- No instalar programas o extensiones de navegadores de fuentes desconocidas ya que estas suelen traer malware el cual puede afectar los dispositivos y extraer la información sensible.
- Evitar el uso de aplicaciones de escritorio remoto que no estén verificadas por la Entidad, estas herramientas pueden crear puertas traseras por medio de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y por lo tanto permitir el acceso a los equipos corporativos.
- Aunque se esté trabajando desde casa, siempre se debe garantizar la seguridad de los datos y cumplir con las políticas de seguridad de la Secretaría Distrital de Movilidad y la Ley de protección de datos personales.
- Las demás instrucciones dadas en este documento.

- La persona funcionaria o contratista debe cumplir con los requerimientos de seguridad de las comunicaciones establecido por la Secretaría Distrital de Movilidad con el fin de evitar afectaciones de capacidades e intrusiones o ataques a la infraestructura tecnológica de la entidad durante la ejecución de su labor como usuario en teletrabajo y/o trabajo en casa. En este sentido los equipos personales deben tener como mínimo antivirus y sistema operativo actualizados y licenciados.

- La persona funcionaria o contratista de la entidad debe tener la responsabilidad de conectarse a internet a través de una red privada, desde su lugar de residencia o el sitio donde se encuentre ubicado para garantizar la conectividad segura desde su equipo o dispositivo personal.

- La persona funcionaria o contratista debe establecer condiciones de seguridad o protección de la información que evite el acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo equipo o dispositivo personal si éste ha sido autorizado previamente por la entidad.

- Para el caso del funcionariado de la entidad que laboran por la modalidad específica de teletrabajo (ley 1221 de 2008) en la cual la entidad ha proporcionado el equipo de cómputo o dispositivo móvil, tal como lo expresa la mencionada ley, “no podrán ser usados por persona distinta al teletrabajador, quien al final del

contrato deberá restituir los objetos entregados para la ejecución del mismo, en buen estado, salvo el deterioro natural".

- Mientras que el funcionariado y/o contratistas estén en acceso a través de VPN a los recursos privados o confidencial de la entidad, no deberán ingresar simultáneamente desde el equipo o dispositivo con el que se conecta, a otros servicios o sitios web como acceso a las diferentes redes sociales, acceso a servicios de streaming de video que puedan generar en la entidad problemas de capacidades que saturen la red corporativa o que puedan causar problemas de ciberseguridad en la entidad. En caso de que el funcionario o contratista de la entidad no cumpla con esta política, su acceso por VPN será restringido.

- Mientras la o el trabajador (a) esté en acceso a través de VPN a los recursos privados o confidencial de la entidad, no deberá ingresar simultáneamente desde el equipo o dispositivo con el que se conecta, a otros servicios o sitios web como acceso a las diferentes redes sociales, acceso a servicios de streaming de video que puedan generar en la entidad problemas de capacidades que saturen la red corporativa o que puedan causar problemas de ciberseguridad en la entidad. En caso de que el funcionario o contratista de la entidad no cumpla con esta política, su acceso por VPN será restringido.

- Para el caso del funcionariado por modalidad de teletrabajo debe estar sujeto a las configuraciones y restricciones que la Oficina de Tecnologías de la Información y Comunicaciones establezca sobre los equipos proporcionados por la entidad, así como las configuraciones de conectividad que igualmente proporciona la Secretaría Distrital de Movilidad al teletrabajador, tal como lo expresa la mencionada ley de teletrabajo en el siguiente texto: "Los empleadores deberán proveer y garantizar el mantenimiento de los equipos de los teletrabajadores, conexiones, programas, valor de la energía, desplazamientos ordenados por él, necesarios para desempeñar sus funciones."

- El contratista que por necesidades personales tenga que salir del país mientras tenga un contrato laboral con la entidad en sus diferentes modalidades deberá informar a la entidad dicho traslado y ubicación de la ciudad para que la entidad pueda tener conocimiento de los accesos desde países del exterior y poder llevar el debido control de seguridad de la información, dados los riesgos y amenazas de ataques de ciberseguridad que pueden proceder de otros países. Así mismo, se debe dar cumplimiento a los anteriores apartados solicitados. Para el caso del funcionariado, el traslado laboral a otros países deberá ser debidamente aprobado por las instancias que la entidad haya considerado pertinente para estos casos.

5.26 Política de Control de Acceso Físico

a. El ingreso a las instalaciones de la Secretaría Distrital de Movilidad debe estar restringido únicamente al personal autorizado.
b. El personal de vigilancia de la Entidad está en la obligación de registrar los dispositivos electrónicos tales como portátiles, torres de computador o video beam, deben ser registrados donde se indique la marca del equipo, el modelo y el serial (o su equivalente) para los funcionarios, funcionarias, contratistas y visitantes. Este registro se realizará al ingreso y a la salida de las instalaciones de la Secretaría Distrital de Movilidad.
c. El ingreso del funcionariado, contratistas o terceros a las instalaciones de la Secretaría Distrital de Movilidad los fines de semana, debe ser avalado previamente por la Subdirección Administrativa.
d. Cualquier ingreso de terceros a las instalaciones de la Secretaría Distrital de Movilidad de lunes a viernes después de las 5:00 p.m., debe ser avalado previamente por la Subdirección Administrativa.
e. Sin excepción, todos los visitantes deben llegar al sitio designado para el registro de visitantes (Recepción de las instalaciones) y ser anunciado por el personal de vigilancia al funcionario y/o contratista a visitar.
f. El registro de visitantes debe incluir el nombre e identificación del visitante, la fecha y hora de entrada y salida del visitante, y el nombre del funcionario o contratista de la Secretaría Distrital de Movilidad que avala el ingreso.

g. Los visitantes deberán ser acompañados por la o el funcionario (a) o contratista de la Secretaría Distrital de Movilidad, que avala el ingreso durante el tiempo que dure la visita.
h. Un visitante no puede avalar el ingreso de otro visitante.
i. En las áreas seguras no se permitirá ningún animal bajo ninguna circunstancia.
j. Los dispositivos electrónicos ingresados por los visitantes tales como portátiles, torres de computador o video beam, deben ser registrados donde se indique la marca del equipo, el modelo y el serial (o su equivalente). Este registro se realizará al ingreso y a la salida de las instalaciones de la Secretaría Distrital de Movilidad.
k. Las y los visitantes que requieran el ingreso a áreas seguras controladas por lectores de tarjetas de acceso, como el centro de datos, deberán solicitar previamente acceso temporal a través del funcionario o contratista que avala su entrada.

5.27 Política de Gestión de Activos de Información, Clasificación y Etiquetado de la Información[25] [26]

Los activos de información de la Secretaría Distrital de Movilidad deben ser identificados, clasificados de acuerdo con los requisitos legales vigentes y valorados frente a los criterios de confidencialidad, integridad y disponibilidad y así determinar el valor de la criticidad de los mismos con el fin de darle el tratamiento adecuado.

a. La información debe ser clasificada por la persona dueña de la información y este a su vez debe informar a la dependencia de la Entidad responsable del proceso de clasificación de manera que se tomen las medidas requeridas para preservar la confidencialidad, integridad y disponibilidad de la misma.
b. Todos los aplicativos o sistemas de información necesariamente deben tener asignado un propietario, el cual es el encargado de definir los niveles de privacidad de la información, así como los usuarios y permisos que cada uno deba tener sobre ella.
c. La persona propietaria de la información es responsable por la actualización de la clasificación de la información de acuerdo con los cambios de la Entidad.
d. La persona propietaria de la información es autónoma de reclasificarla cuando lo considere necesario y debe cambiar del rótulo o etiqueta y notificar a las y los usuarios.
e. Las y los usuarios son responsables de familiarizarse y atender todos los aspectos de la política de seguridad. En caso de existir dudas por parte de las y los usuarios con respecto a la manipulación apropiada de la información, estas deben ser consultadas con la persona custodio o propietario.
f. Es deber de las y los responsables efectuar la clasificación de la información de acuerdo con los patrones definidos por esta política.
g. La información, datos y documentos deben ser claramente etiquetados, de manera que todos las y los usuarios estén enterados de su nivel de clasificación. Para ello se deben seguir los lineamientos establecidos en el instructivo para la clasificación de activos de información PA04-IN03 y deberán ser registrados en el formato de inventario de activos de información de tipo tecnológico PA04-IN03-F02.
h. Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación.
i. Los empleados, contratistas o terceros no pueden utilizar la información reservada o clasificada cuando dejan de trabajar o prestar sus servicios en la Entidad.
j. Destrucción de Información reservada o clasificada: Cuando ya no se requiera una información clasificada como reservada, se deberá realizar la solicitud formal de la destrucción mediante un método aprobado por el responsable del proceso de seguridad de la información de la Entidad.

k. En caso de enviar los equipos a mantenimiento o asignarle el equipo de cómputo a una persona diferente que contenga información reservada o clasificada, la información debe ser borrada de manera que no sea posible su recuperación.

l. Se debe borrar la información reservada o clasificada de los medios magnéticos (discos externos, USB y otros) por un método o programa aprobado por la persona responsable del proceso de seguridad de la información en la Secretaría Distrital de Movilidad. Cuando se requiera deshacerse del medio o equipo, enviar a servicio técnico el mismo o devolver a su proveedor.

m. Los equipos portátiles o dispositivos móviles que contengan acceso a información reservada o clasificada de la Entidad, no pueden almacenar en discos duros sino utilizar almacenamiento en la nube segura definida por la Entidad, para evitar que ante la pérdida del equipo una persona no autorizada pueda acceder a la información.

n. Las y los terceros con los cuales la Secretaría Distrital de Movilidad tenga algún vínculo contractual o comercial, no deben revelar información reservada o clasificada a terceras partes a menos que el originador de la información haya aprobado su revelación y la parte que la reciba haya firmado un acuerdo de confidencialidad.

o. Con el fin de realizar el inventario, la clasificación y etiquetado de los activos de información, los responsables deben utilizar el formato: PA04-IN03-F02 FORMATO INVENTARIO DE ACTIVOS DE INFORMACIÓN DE TIPO TECNOLÓGICO.

p. Este procedimiento se debe actualizar por lo menos una vez al año o cuando se cree un nuevo activo de información como lo indica el instructivo para la clasificación de activos de información PA04-IN03.

q. Al compartir bases de datos con información sensible o reservada, deberá usarse un mecanismo que ayudan a proteger la privacidad llamado anonimización de los datos, es decir, el proceso por el cual se desvincula un dato de interés de un dato personal, hasta el punto de que la identificación personal a partir del dato anonimizado no sea posible mediante “todos los medios que puedan ser razonablemente utilizados”.

5.27.1 Revisión

Las Dependencias responsables de los procesos de gestión documental y gestión de TICS en la Secretaría Distrital de Movilidad deberá realizar periódicamente la revisión y verificación de la información, para

determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

La persona responsable de la información puede revisar y validar en cualquier momento en que el líder del proceso (o quien haga sus veces) así´ lo solicite, o si el equipo de gestión de activos lo solicita a algún líder de proceso o el oficial de seguridad de la información, si así lo requiere.

Las razones por las cuales debería realizarse una revisión o validación son:

- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de un nuevo activo.
- Desaparición de un área, proceso o cargo en la Secretaría Distrital de Movilidad que tenía asignado el rol de propietario (Cambios Organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

5.27.2 Actualización

Una vez se ha definido que´ cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información. Se deben socializar estos cambios, definir el motivo por el cual se hace la actualización y se debe firmar un acta con los cambios realizados de conformidad con el instructivo para la clasificación de activos de información PA04-IN03.

5.27.3 Publicación

El inventario de activos de información debe ser un documento clasificado como “Reservado”, y no debe tener características que lo permitan modificar por los usuarios autorizados. Solo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridad de la información o quien haga de sus veces.

5.27.4 Clasificación de la Información

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. Esta se debe definir de acuerdo con las características de los activos

que se manejan en la entidad y dando cumplimiento con lo establecido en La Ley de Transparencia de la Información (Ley 1712 de 2014), la valoración a tener en cuenta se presenta a continuación:

CONFIDENCIALIDAD	DESCRIPCIÓN
INFORMACIÓN PÚBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN PUBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

5.27.5 Etiquetado de la Información

Para realizar el etiquetado de la de Información se establecerán una serie de ítems que deben ser tenidos en cuenta:

a. Se etiquetará el nivel de clasificación en relación con Confidencialidad, Integridad y Disponibilidad.
b. Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.
c. Para los activos clasificados en confidencialidad se etiquetarán como INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA e INFORMACIÓN PÚBLICA.
d. Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA B.
e. Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA 2 y BAJA 3.

La información a etiquetar por parte de la Secretaría Distrital de Movilidad será aquella que se encuentre dentro del Sistema de Gestión Documental de la Entidad cumpliendo a su vez con la reglamentación vigente aplicable dada por el Archivo General de la Nación.

5.28 Política de Uso Adecuado de los Activos de Información[27]

El uso aceptable de los activos de información de la Secretaría Distrital de Movilidad, implica la aceptación implícita por parte de los usuarios de estos, de las normas, políticas y estándares establecidos para

garantizar la seguridad de la información y el uso de estos, así como de los compromisos y responsabilidades adquiridas.

Los siguientes se consideran actos no autorizados para el uso de los activos informáticos de la Secretaría Distrital de Movilidad y están expresamente prohibidos así:

a. El intento o violación de los controles de seguridad establecidos para la protección de los activos de información de la Secretaría Distrital de Movilidad.
b. Realizar cualquier actividad que pudiera comprometer la seguridad de cualquier activo de información de la Secretaría Distrital de Movilidad.
c. El uso sin autorización de los activos de información de la Secretaría Distrital de Movilidad.
d. El uso no autorizado o impropio de la conexión a la infraestructura tecnológica de las Secretaría Distrital de Movilidad.
e. Intentar evadir o violar la seguridad o autenticación de usuario de cualquier host, red o cuenta.
f. El uso indebido de las contraseñas, firmas digitales o dispositivos de autenticación.
g. Está prohibido a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma.
h. El almacenamiento, instalación, configuración o uso de software ilegal o de datos no autorizados en los activos de información de la Secretaría Distrital de Movilidad.
i. Está prohibido el uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas de información.
j. El hurto, robo, sustracción o uso no autorizado de: datos, información, materiales, equipos y otros elementos pertenecientes a los activos de información de la Secretaría Distrital de Movilidad.
k. Está prohibido retirar de las instalaciones de la Secretaría Distrital de Movilidad o áreas bajo su administración, cualquier activo de información sin previa autorización.
l. El acceso, modificación o alteración no autorizada de componentes, datos o información de los activos de información de la Secretaría Distrital de Movilidad.
m. El uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes de fuentes no certificadas o de terceros sin la previa revisión o autorización de la Oficina de Tecnologías de la Información y Comunicaciones y/o el Oficial de Seguridad de la Información.
n. El servicio de internet puede ser utilizado solamente con fines autorizados y legales. Se prohíbe toda transmisión, difusión, distribución o almacenamiento de cualquier material digital o impreso, en violación de cualquier ley o regulación aplicable. Esto incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, secretos comerciales u otros derechos de prioridad intelectual usados sin la debida autorización, y todo material obsceno o pornográfico, difamatorio o que constituya una amenaza legal.
o. En el uso del correo electrónico, está prohibido: El Spam, el Troll, Mailbombing, reenvió o transmisión de mensajes de carácter no oficial o la suscripción a otro usuario a una lista de correo sin su permiso.
p. Realizar cualquier actividad que pudiera potencialmente traer desprestigio a la Secretaría Distrital de Movilidad.
q. Los mensajes contenidos en los correos electrónicos no pueden ser contrarios a las disposiciones del orden público, la moral, las buenas costumbres nacionales e internacionales y los usos y costumbres aplicables en internet y el respeto de los derechos de terceras personas.
r. Está prohibido el almacenamiento y reproducción de aplicaciones, programas, archivos de audio que no estén relacionados con las actividades propias de las funciones que cumple la

dependencia o el usuario.

s. Las cuentas de red de la Secretaría Distrital de Movilidad operan con recursos compartidos. Está prohibido el uso abusivo de estos recursos por parte de un usuario en una forma tal que afecte negativamente el rendimiento de la misma.

t. Hacer uso de la red de datos de la Secretaría Distrital de Movilidad para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.

u. Enviar información clasificada de la Entidad por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.

v. Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la Secretaría Distrital de Movilidad.

w. Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la Entidad sin la debida autorización.

x. Ingresar a la red de datos de Entidad por cualquier servicio de acceso remoto sin la autorización de la Oficina de Tecnologías de la Información y las Comunicaciones.

y. Usar servicios de internet en los equipos de la Entidad, diferente al provisto por la Oficina de Tecnologías de la Información y las Comunicaciones.

z. Retirar de las instalaciones de la Secretaría Distrital de Movilidad computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.

aa. Entregar, enseñar o divulgar información clasificada de la Secretaría Distrital de Movilidad a personas o entidades no autorizadas.

ab. Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de la Entidad o de terceras partes.

ac. Ejecutar cualquier acción que difame, afecte la reputación o imagen de la Secretaría Distrital de Movilidad, o alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.

ad. Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.

ae. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de Seguridad de la Información.

A continuación, se describen algunas acciones que afectan la Seguridad y privacidad de la Información, y que ponen en riesgo su disponibilidad, confidencialidad e integridad:

a. Dejar los computadores encendidos en horas no laborables.

b. Permitir que personas ajenas a la Secretaría Distrital de Movilidad ingresen sin previa autorización a las áreas restringidas o donde se procese información confidencial.

c. No clasificar y/o etiquetar la información.

d. No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral

e. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.

f. Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.

g. Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos de la Secretaría Distrital de Movilidad para beneficio personal.

h. Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario o contratista.

i. Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
j. Consumir alimentos y bebidas, cerca de la plataforma tecnológica.
k. Conectar a la corriente regulada dispositivos diferentes a equipos de cómputo.
l. Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso.

Cualquier violación o sospecha de violación de las medidas o controles de seguridad de los sistemas de información, o de las políticas de seguridad de la información para la Secretaría Distrital de Movilidad, debe ser reportada inmediatamente por quien conozca de ellas, a la Oficina de Tecnologías de la Información y Comunicaciones y/o al Oficial de Seguridad de la Información, para los fines pertinentes.

5.29 Uso de Internet[28]

Internet es una herramienta de trabajo que permite navegar en sitios relacionados con las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes políticas:

a. La navegación en Internet debe estar controlada de acuerdo con las restricciones de navegación definidas para los usuarios en grupos establecidos por la Oficina de Tecnologías de la Información y Comunicaciones; Los funcionarios y contratistas definidos para los grupos que tengan un perfil de navegación avanzado, serán definidos por la alta dirección y los jefes de área; sin embargo, en ningún caso se considerarán aceptables los siguientes usos:
    - Navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
    - Publicación, envío o adquisición de material sexualmente explícito, discriminatorio, que implique un delito informático o de cualquier otro contenido que se considere fuera de los límites permitidos.
    - Publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
    - Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados por la Oficina Tecnologías de la Información y las Comunicaciones.
    - Publicación de anuncios comerciales o material publicitario, salvo la Oficina Asesora de Comunicaciones y Cultura para la Movilidad cuando lo requiera. Estas solicitudes, deben ser justificadas por el jefe de la Oficina Asesora de Comunicaciones y Cultura para la Movilidad.
    - Promover o mantener asuntos o negocios personales.
    - Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.
    - Uso de herramientas de mensajería instantánea no autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones.

- Emplear cuentas de correo externas no corporativas para el envío o recepción de información institucional.

b. Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por el funcionariado, contratistas y demás terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.

c. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

5.30 Uso del Correo Electrónico[29]

La asignación de una cuenta de correo electrónico de la Secretaría Distrital de Movilidad se da como herramienta de trabajo para cada uno de las y el funcionariado que la requieran para el desempeño de sus funciones, así como a contratistas y otros terceros previa autorización; su uso se encuentra sujeto a las siguientes reglas:

a. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas en la Secretaría Distrital de Movilidad.

b. Los mensajes y la información contenida en los buzones de correo son de propiedad de la Entidad y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo la información y tráfico de esta se considera de interés para la Secretaría Distrital de Movilidad.

c. El tamaño de los buzones y mensajes de correo serán determinados por la Oficina de Tecnologías de la Información y las Comunicaciones.

d. Toda información generada que requiera ser transmitida fuera de la Secretaría Distrital de Movilidad, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables (PDF) y con mecanismos de seguridad (contraseñas). Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

e. Para las cuentas de correo electrónico y el drive corporativo asociado a las cuentas, que la SDM considere que manejan mayor flujo de información y/o información sensible de la Entidad, la OTIC implementará controles de Data Los Prevention (DLP) sobre las mismas, con el fin de monitorear y prevenir la fuga de información corporativa a través de las cuentas de correo electrónico y carpetas compartidas

f. No se considera aceptado el uso del correo electrónico de la Entidad para los siguientes fines:

- Enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Enviar mensajes no autorizados con contenido religioso o político.
- El envío de archivos adjuntos con extensiones como .mp3, .wav, .exe, .com, .dll, .bat, .msi o cualquier otro archivo que ponga en riesgo la Seguridad de la Información; en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones.
- El envío masivo de mensajes corporativos deberá ser solicitado a la Oficina Asesora de Comunicaciones y Cultura para la Movilidad o por el jefe del Área que

lo requiere y debe contar con la aprobación de la respectiva Oficina de Tecnologías de la Información y las Comunicaciones.

g. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la Oficina Asesora de Comunicaciones y Cultura para la Movilidad y deben conservar, en todos los casos, el mensaje legal institucional de confidencialidad.
h. Todo correo electrónico deberá tener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:
    - El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.
    - El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.
    - En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.
    - Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

5.31 Uso de Redes Inalámbricas

a. La Oficina de Tecnologías de la Información y las Comunicaciones definirá los perfiles, horarios, accesos y demás condiciones para la prestación del servicio Wi-Fi al ciudadano.
b. La Oficina de Tecnologías de la Información y las Comunicaciones será la responsable de validar a quien se le asignarán los servicios a través de redes inalámbricas corporativas, así como los perfiles, horarios, accesos y demás condiciones para la prestación del servicio al funcionariado y contratistas en las instalaciones de la Secretaría Distrital de Movilidad.
c. Los usuarios de las redes inalámbricas corporativas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta a identificación, autenticación, control de contenido de internet y cifrado entre otros.
d. En ningún caso se podrá dejar configuraciones y contraseñas por defecto en los equipos inalámbricos.

5.32 Uso de Computación en la Nube

a. Todo el funcionariado o contratistas no tienen permitido almacenar información de la Secretaría Distrital de Movilidad en servicios de alojamiento de archivos multiplataforma en la nube que no hayan sido autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones.
b. Cuando se contraten servicios tecnológicos en la nube, la Oficina de Tecnologías de la Información y las Comunicaciones deberá asegurar el establecimiento de cláusulas contractuales y procedimientos para la protección de la información, definiendo, entre otros, métodos seguros de trasferencia de información, mecanismo fuertes de autenticación, cifrado de información, devolución y borrado seguro de información, acuerdos para la confidencialidad, integridad y disponibilidad de la información. Adicionalmente deberá asegurar que el proveedor de servicios en la nube realice gestión sobre la ciberseguridad en su plataforma y/o servicio.

5.33 Política de Uso de Componentes Electrónicos de Procesamiento de Información.

La asignación de los diferentes recursos tecnológicos se da como herramientas de trabajo para uso exclusivo del funcionariado y contratistas. El uso adecuado de estos recursos se encuentra sujeto a las siguientes reglas:

a. La Secretaría Distrital de Movilidad únicamente a través del personal debidamente autorizado, instalará copias de los programas que han sido adquiridos legalmente en los equipos asignados, en las cantidades necesarias para suplir sus necesidades del servicio. El uso de programas obtenidos a partir de otras fuentes no autorizadas por la Entidad, implica riesgos legales y de seguridad de la información, por lo que dicho uso está estrictamente prohibido. Los funcionarios y contratistas de la Secretaría Distrital de Movilidad, reconocen y aceptan que son enteramente responsables por la utilización de software en sus estaciones de trabajo que no cuente con la respectiva autorización de la Entidad.
b. El uso de dispositivos de almacenamiento extraíbles como DVD, CD, memorias USB, Agendas Electrónicas, celulares, tabletas y teléfonos inteligentes u otros componentes electrónicos que no han sido debidamente autorizados por la Entidad para su uso dentro de su infraestructura tecnológica, pueden implicar riesgos de seguridad de la información cuando se conectan a los computadores. Los usuarios de estos dispositivos deben informarse de los procedimientos formales necesarios para la utilización de estos dispositivos dentro de la Entidad.
c. El software instalado en los equipos de Secretaría Distrital de Movilidad es de propiedad de la Entidad, la copia no autorizada del software de la Entidad o de su documentación, implica una violación a las leyes de derechos de autor y las políticas de seguridad de la información de la Entidad que será tratada mediante los mecanismos legales a los que está sujeta la Secretaría Distrital de Movilidad.
d. La Secretaría Distrital de Movilidad se reserva el derecho de proteger su reputación y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso y las copias no autorizadas de su software e información institucional. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas con propósitos de control interno, control de calidad, atención de incidentes de seguridad de la información o investigaciones. El usuario de equipos conectados a las redes de la Secretaría Distrital de Movilidad reconoce y acepta que su estación de trabajo o dispositivo de comunicación puede ser analizado para evaluar el cumplimiento de las políticas de seguridad de la información de la Entidad.
e. Los equipos de propiedad de la Entidad que se encuentren fuera de las instalaciones de la Secretaría Distrital de Movilidad deben ser protegidos mediante los controles definidos por la Entidad. Los usuarios de dichos equipos se deben informar de los procedimientos formales necesarios para la utilización de estos dispositivos fuera de la Entidad.
f. La instalación de cualquier tipo de software en los equipos de cómputo es responsabilidad exclusiva del Operador Tecnológico o quien haga sus veces, por tanto, son los únicos autorizados para realizar esta labor en la Secretaría Distrital de Movilidad.
g. Ningún activo de información adquirido y que sea configurable, debe ser instalado con la configuración por defecto del fabricante o proveedor, incluyendo cuentas y claves de administrador.
h. Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser autorizados únicamente por la Oficina de Tecnologías de la Información y las Comunicaciones.
i. Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física.
j. Los equipos de cómputo asignados deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando la o el funcionario (a) o contratista responsable de dicho equipo finalice su vinculación con la Secretaría Distrital de Movilidad.[30]
k. Todo componente de procesamiento electrónico de la información debe servir al cumplimiento de los propósitos misionales de la Entidad, el uso por parte de personas, procesos u otros componentes electrónicos de procesamiento de la información debe someterse al uso definido por la Entidad.
l. Todo componente electrónico de procesamiento de la información debe contar con mecanismos que permitan llevar registro y control de las solicitudes de acceso de creación, modificación, inactivación,

bloqueo y eliminación de accesos autorizados al componente electrónico de procesamiento de información.

m. Los siguientes usos se consideran usos no autorizados sobre componentes de procesamiento de información. Los usos no autorizados constituyen un incidente de seguridad de la información:
    - Modificación del componente sin contar con la autorización formal para dichas modificaciones
    - Uso del componente para fines diferentes a los formalmente definidos por la Entidad.
    - Impedir el acceso al componente de procesamiento de información sin justificación real
    - Modificación o Eliminación de los controles de seguridad que protegen al componente de procesamiento de información
    - Todas las acciones sobre el componente de procesamiento de información que sean contrarias a leyes, regulaciones, normas o procedimientos a los que está sujeta la Entidad.

5.34 Política de Protección contra Software Malicioso[31]

a. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información deben estar protegidos mediante herramientas y software de seguridad que previenen el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos dados por código malicioso.
b. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Oficina de Tecnologías de la Información y las Comunicaciones, y deberán ser actualizados permanentemente.
c. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.
d. Todos los medios de almacenamiento que se conectan a equipos de la infraestructura de la Entidad deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la Seguridad de la Información.
e. La Entidad será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.
f. Los sistemas, equipos e información institucionales deben ser revisados periódicamente para verificar que no haya presencia de código malicioso.
g. Los siguientes usos se consideran usos no autorizados del servicio de antivirus y constituyen un incidente de seguridad de la información:
    - Desactivar, eliminar o modificar la configuración de los programas antivirus o de detección de software malicioso en los equipos o sistemas en que estén instalados.
    - Instalar o emplear programas de antivirus no autorizados por la Entidad.
    - Intercambiar o transmitir archivos que hayan sido identificados como infectados por el software antivirus o de detección de código malicioso o sean calificados como sospechosos de estar infectados.
    - Abrir o descargar archivos o documentos que hayan sido identificados como infectados por el software de antivirus o de detección de código malicioso o sean calificados como sospechosos de estar infectados.

5.35 Política de Administración de Backups, Recuperación y Restauración de la información[32]

a. La información de los diferentes procesos, procedimientos y actividades que forman parte de las funciones de la Entidad, se respalda de acuerdo con requisitos legales, nivel de clasificación, períodos de retención documental y requerimientos de uso establecidos en el sistema integrado de gestión de la Secretaría Distrital de Movilidad.

b. Las copias de respaldo de la información deben ser preservadas por el tiempo previamente establecido por las tablas de retención de respaldo de información, resguardando su acceso de acuerdo con su nivel de clasificación y la disposición final definida en las tablas de retención documental de la Entidad.

c. Toda información que soporte procesos, procedimientos o actividades definidas en el sistema de integrado de gestión de la Secretaría Distrital de Movilidad debe tener una definición formalmente documentada de las necesidades de respaldo de información, que debe ser aprobada por el responsable del proceso que incluya mínimo: información a respaldar, periodicidad del respaldo, nivel de clasificación de la información y período de retención de las copias de respaldo.

d. Para todos los sistemas de información que soportan procesos, procedimientos o actividades definidas en el Sistema Integrado de Gestión de la Secretaría Distrital de Movilidad, debe existir documentación formal de las estrategias, procedimientos, estándares y actividades necesarias para la realización operativa del respaldo de la información del sistema.

e. El respaldo de la información almacenada en los equipos de escritorio, dispositivos móviles u otros medios de procesamiento de información diferentes a la infraestructura tecnológica que soporta los sistemas de información de la Secretaría Distrital de Movilidad, debe ser solicitado formal y expresamente a la mesa de servicios de la Entidad a través de correo electrónico mesadeservicios@movilidadbogota.gov.co o el correo electrónico que haga sus veces. Los responsables de la realización de las copias de respaldo evaluarán con la persona solicitante, la estrategia que mejor se ajuste a la solicitud considerando como mínimo: requisitos de negocio, clasificación de la información, necesidades de recuperación y medios tecnológicos disponibles.

f. Todos los sistemas de información que soportan procesos, procedimientos o actividades definidas en el sistema de integrado de gestión de la Secretaría Distrital de Movilidad, deben contar con las herramientas tecnológicas apropiadas que garanticen la realización de las copias de respaldo de considerando los requerimientos de uso de la información, niveles acceso autorizados y períodos de retención definidos por el responsable de la información.

g. Los períodos de retención de la información respaldada se deben definir de acuerdo con los requisitos legales, objetivos de los procesos, niveles de riesgo identificados por los procesos de gestión de riesgos y retroalimentación de las y los usuarios y dueños de la información.

h. Los procedimientos específicos para la realización de las copias de respaldo deben establecer los mecanismos que permitan mantener y realizar trazabilidad de la ejecución de la copia de respaldo, su resultado, responsables, medios usados, información respaldada y trazabilidad de las acciones realizadas durante la ejecución de la copia de respaldo o su restauración.

i. Las copias de respaldo se almacenan en sitios seguros con controles físicos y tecnológicos que permitan el cumplimiento de los estándares mínimos necesarios para preservar las copias durante los períodos definidos, limitar su acceso a los debidamente autorizados y garantizar su disponibilidad cuando el responsable de la información los requiera.

j. Cuando se requiera la ejecución de respaldos que no estén considerados en la estrategia definida, los responsables de los procesos tramitarán su ejecución mediante los procedimientos de gestión de solicitudes de servicio definidos por la Secretaría Distrital de Movilidad

k. Las copias de respaldo se deben someter a pruebas de restauración mensualmente para certificar que cumplen con los propósitos para las cuales fueron realizadas. Los resultados se deben usar para actualizar los procedimientos de respaldo, recursos tecnológicos necesarios, evidenciar oportunidades de mejora o riesgos en la realización de copias de respaldo y

restauración de información. Los responsables de la información deben participar en las pruebas para certificar formalmente que las estrategias de respaldo y restauración se ajustan a las necesidades de sus procesos.

l. Cuando los requisitos legales, requisitos de retención o condiciones de los medios de respaldo de información así lo dictaminen, se debe proceder a la destrucción o disposición final de medio, garantizando que la información contenida en los mismos ya no será accesible. Cuando se requiera destrucción de medios se deben seguir los procedimientos aprobados por el sistema integrado de gestión de la Secretaría Distrital de Movilidad para la preservación del medio ambiente.

m. Los servicios en nube tipo SaaS[33] y PaaS[34] deben contar con un respaldo de información que garantice el cumplimiento de las disposiciones normativas y legales de la información alojada en dichos sistemas de información. Los acuerdos contractuales deben incluir la posibilidad de realizar auditorías de cumplimiento a los respaldos y restauraciones de información.

n. Antes de realizar actividades de mantenimiento preventivo programado es necesario realizar backup completo de la información, esta tarea será realizada por el personal del Operador Tecnológico

5.36 Política de Controles Criptográficos[35]

a. La Secretaría Distrital de Movilidad en cabeza de la Oficina de Tecnologías de Información y las Comunicaciones, vela por que la información digital etiquetada como reservada sea cifrada cuando se transmita, almacene y recibida, garantizando la preservación de la confidencialidad e integridad de la misma.

b. La Oficina de Tecnologías de Información y las Comunicaciones define, implementa y comunica los estándares para la aplicación de controles criptográficos.

c. La Oficina de Tecnologías de Información y las Comunicaciones fija las directrices necesarias para asignar el responsable o responsables de la implementación del sistema criptográfico y el cómo se gestionarán las claves que usa el sistema.

d. La Oficina de Tecnologías de Información y las Comunicaciones vela por que los desarrolladores internos y externos que diseñan, desarrollan y/o implementan sistemas de información, aplicaciones y/o portales donde se maneje información digital reservada, cuenten con mecanismos de cifrado de datos.

e. Se debe verificar que los sistemas de información o aplicativos que requieran realizar transmisión de información reservada, cuente con mecanismos de cifrado de datos.

f. Los certificados de sitio seguro (SSL) y los certificados de firma digital, deben ser emitidos por una Autoridad Certificadora, que garantice la validez de la asociación entre el tenedor del certificado y el certificado en sí.

g. La duración de los certificados de sitio seguro (SSL) y los certificados de firma digital emitidos por la entidad certificadora de la Secretaría Distrital De Movilidad deberán ser mínimo de un año, contados a partir de la emisión. Cuando vencen los certificados estos deben ser revocados y de considerarse necesario, renovados.

h. Se deberán utilizar herramientas para el cifrado de dispositivos removibles. Para implementar este tipo de herramientas se deben tener equipos propiedad de la entidad y que no impacten las operaciones de los usuarios.

i. La Oficina de Tecnologías de Información y las Comunicaciones tendrá en cuenta y dará cumplimiento a la legislación y marcos normativos vigentes cuando se utilizan sistemas criptográficos sobre la información, en especial la ley 594 de 2000 (Ley General de Archivo), la ley 527 de 1999 (Acceso y Uso de Mensajes de datos) y el decreto 1747 de 2000 (Secure Data Colombia), Ley 1273 (Ley de delitos Informáticos, Ley 1581 de 2012 (Protección de Datos

personales) y demás reglamentación que cobije la protección de datos en Colombia , Ley 1712 de 2014 Transparencia de datos, Ley 1581 habeas data.

j. Se deben generar criterios de evaluación sobre el uso de controles criptográficos para la protección de información.

Escenarios de aplicación:

a. Cuando se tenga un dispositivo con información reservada que se encuentre fuera de la Secretaría Distrital De Movilidad se debe aplicar cifrado a los datos.
b. Cuando se envíe un correo electrónico con información reservada.
c. Cuando se tiene un sitio web público en el que todos los usuarios puedan acceder mediante la introducción de nombre de usuario y contraseña.
d. Cuando se tiene un sitio web desde el que se pueda ofrecer un comercio electrónico y que tenga modalidad de pago.
e. Cuando los colaboradores se conectan con la red corporativa desde casa para acceder a los recursos corporativos.
f. Cuando se emitan certificados digitales para garantizar la confianza entre emisor y receptor (Cuando exista entidad certificadora en común).
g. Cuando se emitan llaves de cifrado públicas y/o privadas para realizar transferencia de información reservada entre las partes.
h. Cuando se emitan tokens con firmas digitales para propósitos específicos.

5.36.1 Algoritmos Criptográficos Aprobados

a. Se deberán usar algoritmos criptográficos aprobados por la Oficina de Tecnologías de la Información y Comunicaciones para el uso por Secretaría Distrital De Movilidad que cumplan con:

- Integridad
- Simétricos
- Asimétricos

5.36.2 Protección de las Entidades Certificadoras.

a. Se debe aplicar la plantilla de aseguramiento del sistema operativo.
b. No se debe instalar y ejecutar una entidad de certificación en el mismo sistema donde se hospedan otros roles.
c. No se deben instalar páginas de inscripción web o IIS como parte de una instalación de CA estándar, a menos que sea un requisito empresarial conocido.
d. Las y los administradores que gestionan las operaciones cotidianas de la PKI no deberán usar las mismas cuentas que se utilizan en estaciones de trabajo de productividad personal. Deberán usar cuentas alternativas dedicadas con los permisos necesarios para administrar la PKI.
e. Las CA no contarán tener acceso a Internet, excepto para validar las CRL.

f. Se debe mantener una copia de seguridad limpia de la base de datos de la CA ante la eventualidad de problemas imprevistos o daños en los datos.

5.36.3 Uso de Certificados Wildcard[36]

a. La custodia de la llave privada de los certificados wilcard será responsabilidad exclusiva de la Oficina de Tecnologías de la Información y las Comunicaciones; la cual deberá almacenar las llaves privadas de forma segura restringiendo el acceso a usuarios no autorizados.
b. No debe entregarse el certificado a terceros y mucho menos ser de dominio público, ya que el compromiso de esta puede resultar en eventos de seguridad que afectan directamente a la entidad.
c. La instalación de este tipo de certificados debe realizarse por el custodio, asegurando que la llave privada no quede exportable.
d. En caso de que los dispositivos en los que se instala el certificado no permitan bloquear la exportación de la llave privada, debe garantizarse un perfilamiento de usuarios para que solo el administrador principal de este tenga los privilegios.
e. El certificado Wildcard no debe instalarse en servicios internos o de prueba.
f. Sobre los servicios internos o de prueba se instalarán certificados digitales emitidos desde la CA interna Microsoft.
g. Los certificados digitales (cualquier tipo), no deben ser entregados mediante correo electrónico sin cifrar.

5.37 Política de Gestión de Vulnerabilidades Técnicas[37]

a. La Oficina de Tecnologías de la Información y las Comunicaciones será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la Entidad.
b. Para adquisiciones SaaS[38] y PaaS[39] o cualquier sistema de información tercerizado, se debe incluir la documentación de gestión de vulnerabilidades técnicas y procesos de actualización de los componentes del sistema de información, así como la posibilidad de auditar dichos procesos, con el fin de garantizar el aseguramiento de la información de la entidad.
c. La Oficina de Tecnologías de la Información y las Comunicaciones a través del Operador Tecnológico de la Entidad o quien haga sus veces y el SOC[40]se encargan de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto se hará uso de las herramientas de identificación de vulnerabilidades que consideren necesarias, de uso libre y licenciadas, para la realización de las actividades dentro del análisis de vulnerabilidades.
d. No se permite a los usuarios de los activos informáticos, sin la autorización expresa de la Oficina de Tecnologías de la Información y las Comunicaciones, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos de la Secretaría Distrital de Movilidad, o a la utilización de estos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.
e. Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.
f. La persona responsable de la Seguridad de la Información realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.
g. La persona responsable de la Seguridad de la Información realizará constante verificación de alertas de seguridad emitidas por organizaciones y foros de Seguridad de la Información de

orden nacional y/o internacional, con el fin de verificar la información más reciente que se encuentre disponible respecto a vulnerabilidades y eventos de seguridad que se hayan presentado o que sean susceptibles de ocurrencia.

h. La persona responsable de la Seguridad de la Información realizará las revisiones de las alertas de seguridad informadas por el Operador Tecnológico y dado el caso en que las alertas sean válidas en el entorno de operación de las plataformas tecnológicas asociadas, se deberá definir por parte de dichas oficinas un plan de acción para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

5.38 Política Gestión de Seguridad en las Redes

5.38.1 Controles de Redes

a. La Oficina de Tecnologías de la Información y las Comunicaciones, deberá establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas.
b. La Oficina de Tecnologías de la Información y las Comunicaciones, debe establecer las responsabilidades y procedimientos para la gestión de equipos de redes.
c. Los usuarios de la red interna de la Secretaría Distrital de Movilidad, no pueden realizar o ejecutar acciones en la red que sean exclusivas de los administradores de red.
d. Los funcionarios y contratistas no deben llevar a cabo ningún tipo de instalación de líneas telefónicas, canales de transmisión de datos, equipos tecnológicos para interconexión de equipos en la red, ni cambiar su configuración sin haber sido formalmente aprobados por la Oficina de Tecnologías de la Información y las Comunicaciones.

5.38.2Seguridad de los Servicios de Red

a. La Oficina de Tecnologías de la Información y las Comunicaciones, deberá velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la Secretaría Distrital de Movilidad.
b. La Oficina de Tecnologías de la Información y las Comunicaciones, deberá instalar protección entre las redes internas de la Secretaría Distrital de Movilidad y cualquier red externa con el objetivo de proteger la información de la Entidad de amenazas externas, para lo cual puede utilizar dispositivos de seguridad perimetral tales como firewalls, sistema de detección de intrusos, entre otros.
c. Se debe asegurar de que los proveedores de servicio de redes implementen mecanismos de seguridad.

5.38.3Separación en las Redes

a. La Secretaría Distrital de Movilidad debe considerar la separación de redes que requieran distintos niveles de seguridad y tráfico. Esta separación debe realizarse de acuerdo con la clase de información albergada en los sistemas que constituyen dichas redes. Esto debe incluir equipos de acceso público.
b. La Secretaría Distrital de Movilidad debe separar las redes y los grupos de servicios de información dividiéndolas en dominios lógicos de red, cada uno protegido por un perímetro de seguridad definido.

c. La Secretaría Distrital de movilidad debe establecer un perímetro externo llamado Zona Desmilitarizada (DMZ) en la red a través de la cual se puedan limitar las conexiones desde internet hacia las plataformas informáticas internas, permitiendo la seguridad de las últimas.
d. Cada dominio creado debe ser aprobado por la Oficina de Tecnologías de la Información y las Comunicaciones, y debe ser actualizado en la topología de red de datos de la Entidad.
e. Las redes inalámbricas deben estar separadas de la red principal de usuarios con el fin de minimizar el riesgo en los activos de información. El acceso a estas redes inalámbricas debe ser controlado, debe tener una autenticación segura en los casos que se requiera.

5.38.4 Conexión Remota por Medio de Red Privada Virtual (VPN)

a. La Oficina de Tecnologías de la Información y las Comunicaciones, deberá garantizar que la conexión remota a la red interna de la Secretaría Distrital de Movilidad, debe realizarse a través de una conexión VPN SSL, suministrada por la Entidad.
b. La Oficina de Tecnologías de la Información y las Comunicaciones, deberá establecer métodos apropiados de autenticación, para las y los usuarios que utilicen accesos remotos.
c. Toda solicitud de creación de VPN, debe ser realizada a través del formato autorizado por la Entidad, el cual debe ser aprobado por la o el jefe (a) inmediato del funcionariado o contratista.
d. Al establecer conexiones VPN haciendo uso de equipos ajenos a la Entidad, las y los usuarios entienden y aceptan que sus equipos de cómputo son una extensión de la red de datos de la Secretaría Distrital de Movilidad, y por esta razón deben cumplir con las mismas políticas que aplican para los equipos propiedad de la Secretaría Distrital de Movilidad.
e. Es responsabilidad de las y los usuarios que utilizan los servicios de VPN, asegurar que personas no autorizadas accedan a las redes de datos internas de la Secretaría Distrital de Movilidad.
f. Si la VPN no se ha utilizado en al menos los últimos 90 días, ésta será eliminada. Pasado ese tiempo, en caso de requerirse nuevamente, debe surtir de nuevo todo el proceso para la creación, incluyendo el diligenciamiento del formato respectivo.

5.38.5Sistemas de Acceso Público

a. La información pública producida por las dependencias de la Entidad deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.
b. El portal institucional debe contener la política de privacidad y uso, así como la política de seguridad de este.
c. Toda la información publicada en el portal institucional o cualquier otro medio, deberá contar con la revisión y aprobación de la Oficina Asesora de Comunicaciones y Cultura para la Movilidad.

5.38.6 Publicación de servicios en la DMZ

a. La configuración de la DMZ, incluyendo las reglas del firewall,los controles de acceso y la segmentación de redes, será definida y gestionada por la Oficina de Tecnologías de la Información y las Comunicaciones.

b. La publicación de servicios en la Zona Desmilitarizada-DMZ se realizará siguiendo los principios de seguridad y segregación de redes.

5.38.7 Protección de servicios en VLAN de producción y desarrollo

a. Se prohibe la exposición directa a intranet de los servicios que se encuentren en las VLAN de producción y desarrollo de la Secretaría Distrital de Movilidad.
b. Se deberá implementar la segregación de redes VLAN para aislar los entornos de producción, desarrollo y prueba, limitando el acceso entre ellos y previniendo la propagación de amenazas.
c. Se deberá establecer reglas de firewall y mecanismos de control de acceso para permitir únicamente las conexiones autorizadas a los seravicios en las VLAN de producción y desarrollo.
d. El acceso remoto a los servicios en las VLAN de producción y desarrollo se realizará exclusivamente a través de conexiones VPN seguras, utilizando mecanismos robustos de autenticación y cifrado de datos.

5.39 Política de Administración de Componentes Electrónicos de Procesamiento de Información

a. Todos el funcionariado y contratistas de la Secretaría Distrital de Movilidad responsables de administración de componentes de información están obligados al cumplimiento y seguimiento de esta política y demás políticas de seguridad de la información que adopta la Entidad.
b. Las labores de administración de componentes y servicios de información y tecnología deben estar formalmente documentadas mediante procedimientos que se deben actualizar cuando se presenten cambios sobre dichos componentes o sobre los procedimientos de administración o de operación de dichos componentes o servicios.
c. Las y los administradores y operadores de componentes y servicios de información y tecnología son responsables de generar, mantener, actualizar, preservar y garantizar la seguridad de la información referente a la configuración de los diversos componentes o servicios de información y tecnología.
d. Las modificaciones a los componentes de información y tecnología de la Entidad, deben cumplir con los procedimientos definidos por la Entidad para la gestión del cambio.
e. Las y los administradores y operadores de componentes y servicios de información y tecnología deben reportar mediante los canales autorizados y a las instancias definidas, sin demoras injustificadas cualquier evento que pueda afectar en forma potencial o real la prestación de servicios de información y tecnología de la Entidad.
f. Las y los administradores y operadores de componentes y servicios de información y tecnología son responsables de garantizar y mantener un registro detallado de todos los eventos que sucedan sobre los equipos o servicios a su cargo.
g. Las y los administradores y operadores de componentes y servicios de información y tecnología de la Entidad deben coordinar con las y los dueños de los procesos que usan los componentes y servicios de tecnología las actividades de mejoramiento de los servicios, así como cualquier cambio que afecte los niveles acordados para la prestación de estos
h. Las y los administradores y operadores de componentes y servicios de información y tecnología de la Entidad deben coordinar con la Oficina de Tecnologías de la Información y las Comunicaciones la implementación de todos los controles de seguridad de la información necesarios para el tratamiento de los riesgos de seguridad de la información que se identifiquen sobre los componentes o servicios a su cargo.
i. La Secretaría Distrital de Movilidad se debe encargar a través de la supervisión de los contratos que los administradores de servicios y componentes de información y tecnología deben incluir dentro de sus actividades de gestión mínimo:
    - Mantenimiento y aplicación de las responsabilidades para la administración y operación de componentes, sistemas o servicios a su cargo
    - Mantenimiento y aplicación de los procedimientos necesarios para autorizar las actividades de procesamiento de información sobre los componentes bajo su responsabilidad.
    - Mantenimiento y aplicación de los procedimientos de operación de los equipos o servicios a su cargo.

- Mantenimiento de los acuerdos de confidencialidad sobre la información a su cargo
- Mantenimiento del registro de riesgos de los componentes o servicios a su cargo.
- Mantenimiento y aplicación de los procedimientos que se definan para el acceso de terceros a los componentes a su cargo en situaciones como mantenimiento o garantía.
- Mantenimiento de inventario actualizado de los componentes a su cargo, así como de la configuración detallada de los mismos.
- Mantenimiento de registros del desempeño de los equipos o servicios a su cargo.
- Mantenimiento de registros que muestren las actividades realizadas por los administradores o los operadores de los equipos o servicios a su cargo.
- Mantenimiento de los registros de las fallas sobre los equipos o servicios a su cargo
- Mantenimiento de registros de las y los usuarios a los cuales se les ha otorgado acceso a los servicios o componentes
- Revisión periódica de los privilegios de acceso otorgados a las y los usuarios de los servicios o componentes a su cargo.
- Mantenimiento y aplicación de los procedimientos definidos para asignación de cuentas de usuario y contraseñas de acceso a servicios y componentes
- Revisión periódica de los reportes de análisis de vulnerabilidades que se realicen sobre los equipos a su cargo.
- Implementación y mantenimientos de las medidas de mitigación que se definan para contrarrestar las vulnerabilidades que se identifiquen sobre los componentes o servicios a su cargo
- Mantenimiento y aplicación de los procedimientos de respaldo de la información contenida en los equipos a su cargo.
- Mantenimiento y prueba de los procedimientos de contingencia, recuperación ante desastres y continuidad en la prestación de servicios que se definen.
- Mantenimiento de registros sobre las actividades de atención de eventos, incidentes, problemas e incidentes de seguridad de la información que se presenten sobre los equipos o servicios a su cargo.
- Implementar y mantener los procedimientos que se definan para la asignación, actualización o retiro de los derechos de acceso de las y los usuarios de los componentes o servicios bajo su responsabilidad.
- Implementación y mantenimiento de los controles de protección física lógica o procedimental que se definan para la protección de los componentes o servicios a su cargo brechas.

5.39.1 Seguridad en la Publicación de Servicios

a. Todo servicio publicado en la Zona desmilitarizada-DMZ utilizará puertos y protocolos seguros, como HTTPS para el tráfico web.
b. Se deberán implementar cabeceras de seguridad HTTP para fortalecer la protección de los servicios web contra ataques comunes, como XSS (Cross-Site Scripting) y CSRF (Cross-Site Request Forgery).
c. Se utilizarán certificados digitales válidos emitidos por una Autoridad de Certificación (CA) reconocida para asegurar la autenticidad e integridad de los servicios publicados.

5.40 Política de Adquisición de Hardware

a. La Secretaría Distrital de Movilidad debe seleccionar metodologías para adquisición de hardware que consideren mínimo los siguientes aspectos de seguridad y control:
    - Incluir la seguridad de la información en el ciclo de vida de la adquisición de hardware
    - Hardware compatible con IPv6
    - Garantía tanto del proveedor como del fabricante debidamente documentado
    - Soporte tanto del proveedor como del fabricante debidamente documentado

b. La especificación detallada de los requerimientos de Hardware en los procesos de contratación debe incluir:
    - Identificación y documentación de las funciones específicas que deben cumplir las soluciones de hardware para responder a los requerimientos de la Entidad.
    - Identificación y documentación de los requerimientos de seguridad de la información para cumplir con la normatividad a la que está sujeta la Entidad.
    - Identificación y documentación de requerimientos de infraestructura de información y comunicaciones para el correcto funcionamiento de la solución de hardware.
    - Identificación de los acuerdos de niveles de servicio indispensables para soportar el uso de la solución de hardware.
    - Identificación de cláusulas contractuales para soportar garantías y soporte.

5.41 Política de Gestión de Incidentes de Seguridad de la Información[41]

Un incidente de seguridad de la información es cualquier evento que daña o representa una amenaza seria para toda o una parte de la infraestructura de información y tecnología de la Secretaría Distrital de Movilidad (sistemas de cómputo, sistemas de información, sistemas de telefonía), como pueden ser: ausencia de servicios, inhibición para el uso de sistemas de información, incluyendo cambios no autorizados al hardware, firmware, software o datos, delitos definidos en la ley 1273 de 2009 u otras normas que cobijan a la Entidad, entre otros.

La gestión de incidentes de seguridad de la información de la Secretaría Distrital de Movilidad y sus procedimientos de apoyo definen los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información de la Entidad:[42]

a. Cualquier persona funcionaria de la Secretaría Distrital de Movilidad, contratista o Entidades externas deben reportar eventos relacionados con la seguridad de la información a la Oficina de Tecnologías de la Información y las Comunicaciones de la Secretaría Distrital de Movilidad. La Oficina de Tecnologías de la Información y las Comunicaciones por sí misma también puede identificar incidentes a través de supervisión proactiva de los sistemas de información y tecnología de la Entidad. Una vez identificado el incidente la Oficina de Tecnologías de la Información y las Comunicaciones utilizará los procedimientos internos aprobados para registrar y realizar seguimiento a los incidentes y trabajar con otros funcionarios u organizaciones para tomar las acciones apropiadas como investigar, escalar, remediar, referenciar el incidente a otras organizaciones como lo establecen los procedimientos de respuesta a incidentes de seguridad de la información.
b. Cualquier dispositivo de uso personal como teléfonos inteligentes, computadores portátiles, tabletas, u otros dispositivos de cómputo que estén implicados en incidentes de seguridad pueden ser sometidos a cadena de custodia o protección para fines de investigación o evidencia ante procesos administrativos o legales. En caso de usar estos tipos de dispositivos, sus propietarios aceptan formalmente las políticas de seguridad de la Secretaría Distrital de Movilidad.
c. La Oficina de Tecnologías de la Información y las Comunicaciones es la dependencia responsable por el aislamiento y recuperación de los accesos a sistemas de comunicaciones y

cómputo afectados por el incidente. La Oficina de Tecnologías de la Información y las Comunicaciones debe conformar un equipo para la atención y respuesta a incidentes. De acuerdo con la naturaleza del incidente pueden ser convocados: Niveles directivos de la Entidad, áreas de control interno de la Entidad, equipos jurídicos o técnicos especializados.

d. El plan de respuesta o remediación específico para un incidente puede ser suministrado por requerimiento específico o por iniciativa de la Secretaría Distrital de Movilidad a organismos de seguridad, control o respuesta a incidentes de seguridad del estado con el fin de evaluar su efectividad, solicitar apoyo, demostrar debida diligencia u otros propósitos definidos por la Secretaría Distrital de Movilidad.
e. Cuando sea factible, la Secretaría Distrital de Movilidad adoptará procedimientos para llevar a cabo actividades de prevención de incidentes, supervisión y filtrado de anomalías que puedan afectar a la seguridad de la información o los recursos de información y tecnología de la Entidad.
f. La Oficina de Tecnologías de la Información y las Comunicaciones mantendrá los procedimientos para la respuesta e investigación de los diferentes tipos de incidentes de seguridad de la información, así como asegurar la custodia de las evidencias obtenidas durante la investigación.
g. Todo ell funcionariado y contratistas de la Entidad deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.
h. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.
i. Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

5.42 Política de Traer tu Propio Dispositivo (Bring Your Own Device - BYOD[43])

Esta política aplica a todos los dispositivos electrónicos personales tales como teléfonos inteligentes, tabletas, computadores portátiles que no pertenecen a la Entidad pero que son utilizados por el funcionariado y contratistas que se conecten en las instalaciones de la Secretaría Distrital de Movilidad

Atendiendo a la política general del SGSI con respecto a la responsabilidad de la preservación y protección de la información que todo el personal de la Secretaría Distrital de Movilidad debe cumplir, la entidad no autoriza en primera instancia, el uso de dispositivos BYOD para el almacenamiento de información institucional, sólo se determina mediante procedimientos administrativos en la cual se defina en qué momento se considera viable autorizar uso de dispositivos personales que no sean propiedad de la Entidad para el tratamiento de la información institucional. En este sentido, se debe dar cumplimiento a lo siguiente:

a. Las y los jefes funcionales de cada dependencia de la Secretaría Distrital de Movilidad, serán los responsables de determinar de forma justificada en qué procesos y bajo qué circunstancias se autorizará el uso de dispositivos que no pertenecen la Entidad (BYOD) para almacenar o procesar información institucional pública reservada o información pública clasificada. Así mismo, para dicha autorización la aplicación de las políticas de seguridad requeridas para la información que se almacene y gestione en el dispositivo personal del funcionario o contratista.
b. Los jefes funcionales de las diferentes dependencias responsables de autorizar lo especificado en el ítem anterior, deben identificar y evaluar los riesgos asociados a la divulgación de información pública reservada o información pública clasificada antes de autorizar el uso de los BYOD.

c. La persona funcinaria o contratista tercero al que se autorice un BYOD debe garantizar bajo compromiso de confidencialidad que la información reservada o clasificada correspondiente a sus labores asignadas será almacenada de forma aislada a la información personal que guarde en su dispositivo y debe obligatoriamente cifrar la información de la Entidad de acuerdo con la política de controles criptográficos y controles del sistema de gestión de seguridad de la información. Igualmente debe comprometerse con almacenar la información después de su utilización, en los espacios de almacenamiento corporativos definidos y dispuestos por la entidad a través del Drive del correo electrónico institucional o en carpetas asignadas en la nube corporativa. Posteriormente deberá eliminar toda información privada, confidencial y/o reservada de la Secretaría Distrital de Movilidad que almacenó en su dispositivo BYOD.

d. Todo dispositivo BYOD autorizado para almacenar información de la entidad debe cumplir con la reglamentación vigente en materia de uso de software legal. La o ell usuario (a) es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.

e. En aras de minimizar los riesgos de seguridad de la información que se puedan presentar con la utilización en la red tecnológica corporativa, la Oficina de Tecnologías de la Información y Comunicaciones, deberá realizar periódicamente revisiones técnicas a los equipos BYOD para certificar que están cumpliendo con las políticas de seguridad de la Información. Las revisiones técnicas preservarán el derecho fundamental a la intimidad del usuario del BYOD y las normas sobre Protección de Datos de carácter personal.

f. NOTA: En caso de que la o el funcionario (a) o contratista no esté de acuerdo que se realicen dichas revisiones técnicas a su dispositivo personal no podrá utilizarlo para realizar sus responsabilidades laborales dentro de las instalaciones de la entidad y deberá realizarlos en los dispositivos disponibles que se le asigne para tal fin.

g. La o el propietario (a) del dispositivo BYOD debe aplicar todas las medidas de seguridad razonables que estén a su alcance para preservar la integridad, confidencialidad y disponibilidad de la información que se encuentre en su dispositivo personal.

h. La o el propietario (a) del dispositivo debe informar sin demoras injustificadas a la Oficina de Tecnologías de la Información y Comunicaciones, y a la autoridad competente el robo o pérdida de su dispositivo o de la información contenida.

i. La Oficina de Tecnologías de la Información y Comunicaciones gestionará la pérdida o divulgación de información almacenada en los dispositivos BYOD mediante el procedimiento de gestión de incidentes de seguridad de la información.

5.43 Política de Sincronización de Relojes

La presente política establece mecanismos de sincronización de relojes en los servidores, equipo de cómputo y dispositivos tecnológicos que la SDM determine. Para la sincronización de relojes de la Entidad se dictan las siguientes consideraciones:

- La sincronización de relojes y actividades de los diferentes equipos, aplicaciones o sistemas, es de responsabilidad exclusiva del Operador Tecnológico de la SDM en conjunto con la Oficina de Tecnologías de la Información y Comunicación.
- La sincronización de relojes en servidores, equipo de cómputo y dispositivos tecnológicos, deben establecerse mediante políticas GPO del Controlador de dominio para garantizar una única hora de los sistemas operativos de la Entidad
- Los relojes de los sistemas de información de la SDM deben ser configurados mediante sincronización NTP (Network Time Protocol) de acuerdo con la Hora Legal en Colombia, lo cual debe abarcar servidores, equipos de cómputo y dispositivos tecnológicos vinculados al Directorio Activo de la Entidad.
- En caso tal, de que un sistema de información, servidores o equipo de cómputo deba ser configurado con una zona horaria diferente a la establecida en la presente política, deberá contar con justificación

técnica y ser aprobada por la jefatura de la Oficina de Tecnologías de la Información y las Comunicaciones en conjunto con el Oficial de Seguridad de la Información de la SDM.

5.44 Política de Inteligencia de Amenazas

La Oficina de Tecnologías de la Información y las Comunicaciones debe:

a. Definir las herramientas y fuentes de información para identificar las posibles amenazas cibernéticas que se puedan presentar en la entidad, con el fin de proporcionar una comprensión precisa y detallada del panorama de estas.
b. Recopilar y analizar la información sobre amenazas existentes o emergentes para facilitar acciones informadas que permitan reducir el impacto de dichas amenazas.
c. Implementar acciones correctivas resultado de los análisis de inteligencia de amenazas, que permitan un aprendizaje para enfrentar amenazas futuras.

5.45 Política Gestión de la Configuración

La Oficina de Tecnologías de la Información y las Comunicaciones debe:

a. Definir las configuraciones básicas de seguridad para hardware, software, servicios (por ejemplo, servicios en la nube) y redes, así como para sistemas operativos durante su vida útil y permitir el restablecimiento cuando ocurran cambios en la infraestructura o servicios que las afecten.
b. Revisar y actualizar estas configuraciones de seguridad, de forma preventiva o cuando los proveedores de los equipos indiquen actualizaciones de seguridad recomendadas.

5.46 Política de Filtrado Web

La Oficina de Tecnologías de la Información y las Comunicaciones debe:

a. Establecer y mantener actualizadas las reglas para el uso seguro y apropiado de los recursos en línea, incluyendo cualquier restricción a sitios web y aplicaciones basadas en la web indeseables o inapropiados.
b. Definir lineamientos y controles para restringir el acceso a sitios web que contengan información ilegal o que se sepa que contiene virus o material que pueda afectar los equipos de la entidad, se debe considerar bloquear el acceso a los siguientes tipos de sitios web:

- Sitios web que tienen una función de carga de información a menos que esté permitido por razones comerciales válidas.
- Sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing).
- Servidores de comando y control.itio web malicioso adquirido a partir de inteligencia de amenazas.
- Sitios web que comparten contenido ilegal

c. Controlar el acceso a contenidos no autorizados (redes sociales como: Facebook, Twitter, YouTube y similares, páginas o servicios de internet no permitidos) salvo excepciones como el ejercicio de las actividades propias del proceso con previa autorización del Jefe Inmediato indicando el recurso al cual requiere acceder, el tiempo y justificando las razones por las cuales se solicita.

5.47 Política de Enmascaramiento de datos

La Oficina de Tecnologías de la Información y las Comunicaciones debe:

a. Seleccionar y aplicar alguna de las técnicas para efectuar el enmascaramiento de datos: anular o eliminar algunos caracteres, sustitución de valores, reemplazos con su hash u ofuscación de datos; para ocultar

datos personales, sensibles y/o confidenciales de las bases de datos de producción.

b. Seleccionar y aplicar alguna de las técnicas para efectuar el enmascaramiento de datos: anular o eliminar algunos caracteres, sustitución de valores, reemplazos con su hash u ofuscación de datos; para ocultar datos personales, sensibles y/o confidenciales de las bases de datos de producción.

c. En caso de requerirse información para el ambiente de pruebas, validar que la información que sea entregada a los desarrolladores para la ejecución de pruebas se encuentre enmascarada (ofuscación) y no revelar información confidencial de los ambientes de producción.

El funcionariado y colaboradores de la entidad deben:

Reportar a la Oficina de Tecnologías de la Información y las Comunicaciones los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados a la identificación de titularidad en información personal.

5.48 Política de Eliminación de la Información

La Oficina de Tecnologías de la Información y las Comunicaciones a través del Operador Tecnológico de la entidad o quien haga sus veces debe:

a. Aplicar medidas específicas de eliminación segura, garantizando un tratamiento adecuado de los datos críticos.

b. Eliminar la información en sistemas de información, aplicaciones y servicios que no sea de valor para los procesos de la entidad, con autorización del líder del proceso o propietario de la información.

c. Utilizar mecanismos de eliminación apropiados para el tipo de medio de almacenamiento que se va a eliminar.

d. Eliminar la información confidencial cuando el equipo se devuelve a los proveedores, asegurándose de conservar la información por el tiempo necesario para su resguardo.
e. En la reasignación y reutilización de equipos de cómputo se debe realizar un borrado seguro de la información con el fin de evitar acceso no autorizado a la información.

5.49 Política de Prevención de Fuga de datos

a. La Oficina de Tecnologías de la Información y las Comunicaciones debe reducir el riesgo de fuga de información analizando las situaciones en las que se requiere restringir la capacidad de determinados usuarios para cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la organización.
b. La copia o transferencia por cualquier medio electrónico de Información pública Clasificada o Pública Reservada debe estar autorizada y controlada por el propietario de la información.

5.50 Política de Actividades de Seguimiento

La Oficina de Tecnologías de la Información y las Comunicaciones debe:

a. Establecer los métodos y herramientas adecuadas para el monitoreo de las redes, infraestructura, sistemas y aplicaciones soportados en la plataforma tecnológica de la entidad.

b. Monitorear permanentemente los eventos de las plataformas tecnológicas de la entidad que puedan generar un incidente de seguridad y privacidad de la información y que atente contra la confidencialidad, integridad y disponibilidad de los activos de información.

c. Bloquear actividades o eventos identificados que no correspondan a una acción válida o acorde a las funciones de una dependencia, sin perjuicio de iniciar procesos legales internos o externos a que haya lugar.

5.51 Política de Instalacion de software en sistemas operativos

La Oficina de Tecnologías de la Información y las Comunicaciones debe:

a. Establecer restricciones y limitaciones para la instalación del software en los equipos de cómputo de la entidad, según el licenciamiento disponible.

b. Realizar el análisis del requerimiento de instalación de software de uso libre en términos de seguridad de la información, tomando la decisión de aprobación o no de la solicitud.

c. Conceder accesos temporales y supervisar a los fabricantes y terceros autorizados, para realizar actualizaciones sobre el software.

d. Verificar que los administradores de la plataforma tecnológica ejecuten las actualizaciones a nivel de software previamente autorizadas en el comité de cambios.

El funcionariado y colaboradores de la entidad deben:

a. Utilizar el software legalmente adquirido, desarrollado y/o autorizado por la entidad.

b. En caso de requerirse la instalación de software de uso libre se debe remitir solicitud a través de la mesa de servicios establecida en la entidad; relacionando el nombre de la aplicación, la versión, el tipo de licencia de uso, la casa de software productora, la justificación del requerimiento y el periodo de tiempo estimado de uso, con autorización del Jefe de la dependencia.

ELABORÓ	REVISÓ	APROBÓ
Jasvleidy Fajardo Rozo Profesional Especializado(a) 222-19	Lady Carolina Cardenas Perez Contratista	Edgar Eduardo Romero Bohorquez Jefe(a) de Oficina

Jasvleidy Fajardo Rozo @ 2024-11-19, 11:43:59