FORMATO - INDUCCIÓN

Transporte

SEGURIDAD DE LA INFORMACIÓN GTI-F-026

Sistema de Gestión de Seguridad de la Información

Bienvenido(a) al Ministerio de Transporte, este documento contiene la información que debes conocer respecto a la **Seguridad de la Información** de la Entidad.

¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La seguridad de la información consiste en todo el conjunto de políticas, manuales, procedimientos y controles que se implementan en una entidad con el objetivo de proteger la **CONFIDENCIALIDAD**, **INTEGRIDAD** Y **DISPONIBILIDAD** de los **ACTIVOS DE INFORMACIÓN**.

La **CONFIDENCIALIDAD** de un activo, significa que solo quienes estén autorizados tengan el acceso a dicho elemento.

La **INTEGRIDAD**, indica que los activos no sean modificados o alterados por personas no autorizadas.

La **DISPONIBILIDAD**, indica que los activos puedan ser usados o accedidos siempre que se necesiten.

Un **ACTIVO DE INFORMACIÓN**, es todo aquello que genera, transmite, almacena o procesa información en una entidad. En ese orden de ideas los activos de información pueden ser, entre otros los siguientes:

- Aplicaciones de la entidad
- Hardware
- Redes
- Información Física o Digital
- Infraestructura Física
- Personas

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Un Sistema de Gestión de Seguridad de la Información, permite planificar, implementar, evaluar y mejorar continuamente los diferentes componentes de la seguridad (Políticas, manuales, controles, indicadores) con el objetivo de reducir a la menor probabilidad posible, la afectación de los activos de información. Su alcance está definido para todos los procesos de la entidad.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Es la base de todo el sistema, es la declaración principal del Ministerio de Transporte donde indica su compromiso en la protección de los activos de información dada su importancia para la misión institucional. TODOS debemos conocerla y cumplirla.

"*El Ministerio de Transporte establece la presente Política Institucional de Seguridad de la Información y la Ciberseguridad mediante la cual expresa su compromiso de cumplir los requisitos definidos en el marco del estándar internacional ISO/IEC 27001 en su versión más reciente y del Modelo de Seguridad y Privacidad de la Información, para adoptar, implementar, operar, mantener, evaluar e impulsar la mejora continua del sistema de gestión de seguridad de la información y ciberseguridad, propendiendo porque el comportamiento personal y profesional de los funcionarios, contratistas y terceros sobre la información obtenida, generada o procesada por el Ministerio, mantenga los niveles de confidencialidad, integridad y disponibilidad requeridos desde los diferentes procesos institucionales, a través de la adecuada gestión de sus activos de información, de los riesgos valorados y de los incidentes que sean identificados.*"

Igualmente, la política traza 5 objetivos que se buscan lograr, a través de la implementación del SGSI:

- *Gestionar adecuadamente los riesgos de seguridad digital del Ministerio.*
- *Establecer lineamientos de acuerdo con las necesidades del Ministerio y del SGSI.*
- *Fomentar la cultura de seguridad de la información.*
- *Gestionar los eventos e incidentes de seguridad*

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL BUEN USO DE LOS ACTIVOS DE INFORMACIÓN.

Estos son los lineamientos que todo el personal del Ministerio de Transporte debe seguir, para proteger los activos de información desde diferentes ámbitos:

ESCRITORIO LIMPIO

- No dejes archivos digitales en el escritorio de tu pantalla.
- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Las estaciones de trabajo deberán apagarse al final de la jornada.
- Los computadores portátiles deben estar con un cable de seguridad o deben almacenarse dentro de los cajones del escritorio.
- Los puestos de trabajo deben permanecer limpios y ordenados y

- *Mejorar de manera continua el sistema de gestión de seguridad de la información y ciberseguridad del Ministerio***.**

Además de lo anterior en la Política General encontrarás los roles y responsabilidades de todos los funcionarios y contratistas de la entidad y otros lineamientos importantes,

no debe existir información sensible desatendida.
- Las llaves utilizadas para asegurar los cajones con información sensible no deben dejarse desatendidas.
- Tableros con información sensible deben ser borrados una vez se ha finalizado su uso.
- Los documentos que contengan información sensible y requieran ser eliminados se debe realizar mediante métodos seguros para tal fin.
- En razón al respeto con los compañeros de oficina y por razones de protección a los dispositivos tecnológicos, no está permitido el consumo de alimentos y bebidas en los puestos de trabajo.

USUARIOS Y CONTRASEÑAS

- La creación y modificación de usuarios y contraseñas en la infraestructura tecnológica son responsabilidad de la persona designada por el Grupo de

ENCUENTRA LA POLÍTICA COMPLETA EN EL SIGUIENTE QR CON TU CELULAR.

Tecnologías de la Información y las Comunicaciones.
- La creación, modificación, bloqueo temporal o cancelación de las cuentas de usuario están sujetas a una solicitud formal emitida por el Líder de Proceso o jefe de Dependencia.
- Las credenciales de usuario son de uso personal e intransferible.
- Las contraseñas deben cambiarse cada 60 días.
- Crea contraseñas de MÍNIMO 8 caracteres.
- No uses datos personales o fácilmente reconocibles para tus contraseñas.
- Debes utilizar mayúsculas, minúsculas, números y caracteres especiales para crear tu contraseña segura.
- Las contraseñas o credenciales de acceso no deben escribirse en memos o notas o documentos que puedan encontrarse a la vista de los demás usuarios.
- Está prohibido facilitar o proporcionar acceso a las

aplicaciones e información a usuarios o a terceros no autorizados a través de las credenciales de acceso otorgadas.

USO DE INTERNET

- No se permite la descarga e instalación de software, música o videos.
- Está prohibida la navegación a sitios de pornografía, drogas, terrorismo, segregación racial o religiosa, hacking entre otras.
- No está permitido el intercambio de información clasificada y/o reservada del Ministerio de Transporte con terceros.
- No se permite el acceso a portales de intercambio y almacenamiento de archivos en la nube como DropBOX, BOX, Mega, Wetransfer, entre otros que no se encuentren autorizados.
- Se prohíbe el uso de tecnologías "puente" o intermediarias como "proxies" o "acceso por webproxies", así como cualquier página o mecanismo que intente omitir o violar las políticas de seguridad del Ministerio.
- No está permitida la reproducción de video/streaming relacionados con entretenimiento o que no estén asociados con el desempeño de las funciones del Ministerio de Transporte.
- Este servicio no puede ser usado para beneficios personales o para adelantar actividades de comercio electrónico, o para realizar proselitismo político o religioso.
- No serán permitidas páginas como Outlook, Gmail, Facebook, Instagram o redes sociales, a menos que su labor amerite la excepción.

USO DE CORREO ELECTRÓNICO

- Los buzones del correo corporativo y su contenido pertenecen al Ministerio de Transporte.
- Debe usarse estrictamente para asuntos institucionales (no personales).
- No está permitido enviar cadenas, videos, música, programas o ejecutables.
- Solamente se deben emplear los formatos de firmas estipuladas.

USO DE RECURSOS TECNOLÓGICOS

- No está permitido modificar los dispositivos o equipos proporcionados.
- No puedes instalar software NO AUTORIZADO en los equipos de cómputo.
- No está permitido escanear o atacar las redes, sistemas o equipos del Ministerio. Si necesitas algo, el grupo TIC revisará tu solicitud, no hagas cosas por tu cuenta.
- Solamente el Grupo TIC puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de TI.
- Los funcionarios no deben realizar cambios en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física o lógica y demás, sólo podrán ser realizados por el Grupo TIC.
- Las unidades de CD, DVD, dispositivos USB o unidades extraíbles, estarán deshabilitadas en todas las estaciones de trabajo.
- No está permitido el uso de medios removibles en equipos que estén conectados a la red corporativa del Ministerio de Transporte.
- El Grupo TIC será la única dependencia encargada de la adquisición e implementación de software y hardware.

TRAE TU PROPIO DISPOSITIVO "BYOD"

- En principio, esta los colaboradores que se encuentran vinculados al Ministerio de Transporte mediante un contrato de prestación de servicios y a los funcionarios que estén debidamente autorizados por los jefes de dependencia y GTIC.
- Se debe contar con la autorización explícita de poder hacer uso del dispositivo al interior de alguna de las sedes del Mintransporte, y para ello, se deberá hacer un registro de

ingreso y salida en las porterías de cada sede y o piso.

- El usuario acepta las condiciones y políticas internas de uso de los servicios de interconexión del Mintransporte.
- El propietario del dispositivo acepta que el tráfico que genera podrá ser monitoreado y en los casos en donde se identifique potenciales riesgos de seguridad, podrá ser desconectado de ella.
- Las licencias de software tanto de sistemas operativos como programas específicos que estén instalados en el dispositivo, son propiedad y responsabilidad del propietario del dispositivo y asume toda responsabilidad por irregularidad relacionada con la propiedad intelectual de estos.
- La responsabilidad por la seguridad física del dispositivo es del propietario de este, y en ningún caso el Ministerio se hará solidario por daños o pérdidas de dicho dispositivo.
- Al terminar la relación contractual o laboral o la actividad específica para el cual fue ingresado, el dispositivo deberá ser sometido a un proceso de desvinculación de los servicios institucionales y de borrado seguro de la información del Ministerio que se haya almacenado en estos.

MANEJO DE INFORMACIÓN

- Todo activo que repose en los recursos TIC asignados por el Ministerio es de propiedad de la Entidad. (Toda la información sea cual sea pertenece a la Entidad y no a los funcionarios o colaboradores de la misma).
- No pueden retirarse los activos de información, sin previa autorización del dueño del activo, estas autorizaciones deben quedar por escrito.
- Los activos de información almacenados en los recursos TIC o que se encuentren en medios físicos (Documentos) asignados al personal del Ministerio deberán ser usados solo para los fines que fueron creados u obtenidos, según los lineamientos de clasificación y etiquetado que se encuentren vigentes.
- No se debe almacenar música, videos o información personal, netamente debe guardarse información laboral.
- Leer el índice de información clasificada y reservada, para entender la importancia de la información y el manejo que debe darse a determinados activos.
- Utilizar el fileserver para respaldar información relevante para las funciones.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Todos los funcionarios y/o contratistas tienen el deber de reportar los incidentes de seguridad de la información (robo, hurto, modificación, sustracción, acceso no autorizado a los activos de información), esto tendrá absoluta reserva.
- El grupo TIC podrá revisar registros de auditoría sobre tus accesos, navegación hacia internet, para velar por el cumplimiento de las políticas.
- Se pueden reportar los incidentes por distintos medios de comunicación al grupo TIC (Correo Electrónico o Mesa de Servicios).
- Los reportes recibidos por parte del Grupo TIC serán tratados como confidenciales y con absoluta reserva, cualquier falla en este atributo podrá ser sancionada.

DEVOLUCIÓN DE LOS RECURSOS TECNOLÓGICOS

- La devolución de los recursos tecnológicos debe realizarse en todos los casos en donde se presente una terminación del vínculo laboral (para los colaboradores de planta) o del contrato de prestación de servicios (para los contratistas de prestación de servicios).

- También se deberá realizar el proceso de devolución de dispositivos, en aquellos casos en donde se realice un cambio administrativo en la planta de personal tal como una promoción en el cargo, ascenso, o el nombramiento en un encargo temporal.
- En todo caso, cualquier equipo y/o dispositivo que el Ministerio le haya asignado al colaborador, se debe devolver en las mismas condiciones operacionales en que le fue suministrado.
- Será responsabilidad del colaborador, generar una copia de seguridad de la información contenida en los diversos dispositivos antes de devolverlos al almacén y deberá entregar un ejemplar de dicha copia al jefe inmediato y al proceso de gestión documental. La copia puede ser generada con el apoyo de la Mesa de Servicios de TI, a través de los conductos dispuestos para hacer solicitudes.
- En caso de haber configurado claves de acceso o cifrado parcial de archivos o directorios, se deben entregar estas claves para poder abrir la información correspondiente o se debe eliminar esta protección antes de ser devueltos.

SANCIONES

- Se aplicarán sanciones de acuerdo con el Código Único Disciplinario según corresponda o los procedimientos administrativos a los que haya cabida.
- El incumplimiento de las políticas de seguridad de la información dará lugar a la aplicación de sanciones administrativas previstas por la Código Único Disciplinario, sin perjuicio de la responsabilidad penal a que haya lugar.
- Grupo TIC será el encargado de recopilar y entregar a la Oficina de Control Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para la determinación de la sanción, así mismo será el encargado de gestionar el Incidente de seguridad.

REVISA EL MANUAL COMPLETO EN EL SIGUIENTE QR

CERTIFICACIÓN Y ACEPTACIÓN

Con base al presente documento, certifico con mi nombre, firma y mi identificación que he leído y tengo pleno conocimiento de las políticas de seguridad de la información del Ministerio de Transporte, así mismo de las posibles sanciones en caso de incumplimiento de los lineamientos allí descritos.

NOMBRE: Andrea Judith Gómez Díaz

FIRMA: 

CÉDULA: 1052953875

FECHA: 5 de enero de 2026