Gestión de Tecnologías de la Información y Comunicaciones

Política de Seguridad de la Información

Código: GTIC-POL-001

Versión: 01

Marzo 2023

Sistema Integrado de Gestión

Tabla de contenido

1. Introducción

Para la OPERADORA DISTRITAL DE TRANSPORTE La adopción de un sistema de gestión de la seguridad de la información (SGSI) es una decisión estratégica, que nos permitirá como entidad mitigar los riesgos de la información de carácter misional, tomando como base los controles y requisitos identificados en el estándar ISO/IEC 27001:2013, acuerdos contractuales y regulaciones legales.

El sistema de gestión de la seguridad de la información nos permitirá preservar la confidencialidad, integridad y disponibilidad de la información, contemplando procedimientos adecuados de planificación e implementación de controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de estos.

El presente documento describe la política SGSI definida por la OPERADORA DISTRITAL DE TRANSPORTE como insumo y base para la implantación de los controles, procedimientos, guías y estándares definidos, por lo que su conocimiento y actualizaciones se dará a conocer a todos los funcionarios internos o externos que tengan relación con la entidad.

2. Objetivo

Establecer una adecuada gestión a los riesgos de seguridad de la información, para garantizar la confidencialidad, integridad y disponibilidad de los activos de información, que deben seguir todos los funcionarios directos, contratistas, proveedores o cualquier persona que tenga una relación contractual con la OPERADORA DISTRITAL DE TRANSPORTE.

3. Aplicación Responsables

3.1 Responsables de Seguridad de la Información

- Velar por el cumplimiento de lo consignado en estas directrices y su aplicación en los sistemas de información de la entidad.
- Se deberán realizar revisiones periódicas mediante las cuales se evidencie la adecuada aplicación de controles en la infraestructura física y lógica.
- Se deberá comunicar y socializar las políticas de seguridad de la información a todos los funcionarios o como contratistas y proveedores.

3.2 Gerencia de Recursos Humanos

- Realizar la ejecución de las actividades relativas a la seguridad de la información en los procesos de selección, durante la ejecución del empleo y luego de la terminación

contractual en el momento de desvinculación, que se realicen de acuerdo con la política de seguridad implementados de la entidad.

- Asegurar que los empleados comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
- Informar a todo el personal que ingresa, sus obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información.
- Dar a conocer los acuerdos de Confidencialidad con funcionarios

3.3 Funcionarios, contratistas y terceros (partes interesadas externas)

- Cumplir con las políticas de Seguridad y Privacidad de la Información, contempladas en el presente documento.
- Reportar de manera a la oficina de TI o al líder del área, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.
- Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.
- Utilizar únicamente software y demás recursos tecnológicos autorizados.

4. Definiciones[1]

- **Acción correctiva:** Acción para eliminar la causa de una no conformidad y prevenir su repetición.
- **Acción preventiva**: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.
- **Aceptación del riesgo:** Decisión informada de asumir un riesgo.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Alcance:** Ámbito de la organización que queda sometido al SGSI.
- **Alta dirección:** Tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización. Si el alcance del sistema de gestión cubre solo una parte de una organización, la alta dirección se refiere a aquellos que dirigen y controlan esa parte de la organización. A la alta dirección a veces se le llama gerencia ejecutiva y puede incluir

[1] https://www.iso27000.es/glosario.html

directores ejecutivos (CEO), directores financieros (CFO), directores de información (CIO) y funciones similares.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.
- **Autenticación:** Provisión de una garantía de que una característica afirmada por una entidad es correcta.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.
- **Control de acceso:** Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.
- **Corrección:** Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.
- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Eficacia:** Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.
- **Evento de seguridad de la información:** Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.
- **Fiabilidad:** Propiedad del comportamiento y de unos resultados consistentes previstos.
- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

- **Monitoreo:** Determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.
- **No conformidad:** Incumplimiento de un requisito.
- **Objetivo:** Puede ser estratégico, táctico u operativo. Los objetivos pueden relacionarse con diferentes disciplinas (como las metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, de toda la organización, proyecto, producto y proceso). Un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de seguridad de la información o mediante el uso de otras palabras con un significado similar (por ejemplo, propósito, meta o hito).
- **Organización:** Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.
- **Política:** Intenciones y dirección de una organización, expresada formalmente por su alta dirección.
- **Proceso:** Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
- **Riesgo:** El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.
- **Sistemas de Gestión:** Puede abordar una sola disciplina o varias disciplinas. Los elementos del sistema incluyen la estructura, roles y responsabilidades, planificación y operación de la organización. El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.
- **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.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. Marco de Referencia

5.1 Referencias Normativas

- Ley 1273 de 2009: En el que se reglamentan la “Protección de la Información y de los Datos”.
- Resolución Distrital 305 de 2008 de la Comisión Distrital de Sistemas, por la cual se expiden políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
- Decreto 2573 de 2014: En el que se reglamentan los lineamientos generales de la estrategia de gobierno en línea.
- Decreto Distrital 591 de 2018. En el que se adopta el Modelo Integrado de Planeación y Gestión Nacional y se dictan otras disposiciones.
- Decreto Distrital 807 de 2019 Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones.
- Resolución Distrital 305 de 2008 de la Comisión Distrital de Sistemas, por la cual se expiden políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
- Sentencia T-444 de 1992: recolección de información por parte de los organismos de seguridad del Estado.
- ISO-IEC-27001: Sistema de Gestión de Seguridad de la Información “SGSI”.
- ISO-IEC-27002. Código de prácticas para controles de la información.

  ISO-IEC- 27005. Guías sobre la gestión de riesgos”.
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL

6. Políticas Específicas de Seguridad de la Información

6.1 Política para dispositivos móviles[2]

Control:	A.6.2.1 Política para Dispositivos Móviles
Objetivo:	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, hagan uso de dispositivos móviles en la entidad

Lineamientos:

- Los funcionarios que hagan uso de dispositivos móviles no deberán tener información privada respecto de la información institucional, esto cuando la información este contenida en un mismo dispositivo móvil.
- Para el uso de dispositivos cualquiera que este sea 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.

6.2 Política Clasificación de la información[3]

Control:	A.8.2 Clasificación de la información
Objetivo:	Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, hagan uso de cualquier tipo de información relacionada con el objeto misional de la entidad.

Lineamientos:

6.2.1 Gestión de los activos de la información

Los activos de la información de la Operadora Distrital de Transporte que se generen procesen, almacenen y/o transfieren, deben ser clasificados con su nivel de criticidad y según su naturaleza de seguridad de la información, de la siguiente manera:

[2] ISO/IEC 27001:2013 Anexo A, Ítem 6.2.1
[3] ISO/IEC 27001:2013 Anexo A, Ítem 8.2

Confidencialidad	Disponibilidad	Integridad
Confidencial	Alta	Alta
Uso exclusivo ODT	Media	Media
Pública	Baja	Baja

6.2.2 Pilar de la confidencialidad

Confidencial: Información de la entidad que solo debe ser accesible a un grupo reducido de personas o a las áreas gerenciales. En caso de ser conocida, utilizada o modificada por personas no autorizadas impactaría de manera grave a la entidad, como lo seria afectación en el ámbito legal o perdida de imagen.

- La información clasificada en este ítem será cifrada.
- Solamente la persona dueña de la información o con permiso a la misma, perteneciente al dominio “odt.gov.co” y autenticada en Office 365 podrán acceder a esta información.

Uso exclusivo ODT: Información de conocimiento general de la ODT, utilizada de manera transversal en el momento que sea requerido por cualquier usuario perteneciente a la entidad. En caso de ser conocida, utilizada o modificada por personas ajenas de la entidad sin previa autorización impactaría de manera media a la entidad.

- La información clasificada en este ítem será cifrada.
- Solamente las personas pertenecientes al dominio “odt.gov.co” y autenticada en Office 365 podrán acceder a esta información.
- El dueño de la información puede autorizar a otros usuarios internos y externos acceso a la información, estableciendo si da permisos de lectura y/o escritura.

Pública: Esta información puede ser compartida, entrega o publicada sin ninguna restricción a terceros, funcionarios o cualquier persona sin ocasionar daños o perjuicios a la entidad.

- La información no se cifra
- Cualquier persona puede acceder a ella.

6.2.3 Pilar de la disponibilidad

- **Alta:** La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar perdidas de imagen graves a entes externos.
- **Media**: La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar perdidas de imagen moderadas a entes externos.

- **Baja:** La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de perdida de imagen.

6.2.4 Pilar de integridad

- **Alta:** Información cuya perdida de exactitud y completitud puede conllevar a un impacto negativo de índole legal o económico, retrasar sus funciones, o generar perdidas de imagen graves de la entidad.
- **Media:** Información cuya perdida de exactitud y completitud puede conllevar a un impacto negativo de índole legal o económico, retrasar sus funciones, o generar perdidas de imagen moderado a funcionarios de la entidad.
- **Baja:** Información cuya perdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.

6.3 Política Control de acceso[4]

Control:	A.9 Control de acceso
Objetivo:	Limitar el acceso a los recursos de tratamiento de la información y a la información.
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, hagan uso de cualquier tipo de sistema de información relacionada con el objeto misional de la entidad.

Lineamientos:

6.3.1 Acceso a los sistemas de la información

- El acceso a los sistemas de información de la Operadora Distrital de Transporte sea desde la red corporativa o redes diferentes, deber ser únicamente para el desarrollo de las actividades propias a las funciones correspondientes a su cargo, por parte de TI se habilita acceso básico de acuerdo con el área a la que pertenece el colaborador, cuando se requieran accesos específicos debe crear un caso por la mesa de ayuda de Odoo. El acceso básico debe darse bajo el principio de cada usuario, solo debe tener acceso a lo que necesita conocer teniendo en cuenta la clasificación de la información, con el fin de editar el acceso no autorizado de personas o usuarios que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

[4] ISO/IEC 27001:2013 Anexo A, Ítem 9

6.3.2 Acceso a Redes Inalámbricas

- El área de TI 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 a los funcionarios y contratistas en las instalaciones de la OPERADORA DISTRITAL DE TRANSPORTE.
- 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.

6.4 Política de cuentas de usuario[5]

- El uso de la cuenta de usuario es responsabilidad única y absoluta del funcionario al cual se le asigne.
- La cuenta es de uso personal e intransferible, no se debe compartir con nadie, en ningún caso se debe realizar préstamo de usuarios o permitir que otros hagan uso de la cuenta asignada.
- Toda cuenta de usuario debe estar protegida, mediante contraseña que cumpla los requisitos mínimos de seguridad establecidos en el numeral 6.5 Políticas de contraseña del presente documento.
- En ningún caso, se deben exponer las contraseñas de usuario en lugares visibles o de fácil acceso a terceros.
- Todos los sistemas de información que requieren la configuración de una cuenta de administración son responsabilidad del área de TI y deben ser operados cumpliendo con todas las políticas de seguridad establecidas en el SGSI.

Control:	A.9.2 Gestión de Acceso de usuario
Objetivo:	Garantizar el acceso o de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, hagan uso de cualquier tipo de sistema de información relacionada con el objeto misional de la entidad.

Lineamientos:

[5] ISO/IEC 27001:2013 Anexo A, Ítem 9.2

6.4.1 Creación de cuentas de usuario

Todas las cuentas de usuario que vayan a ser usadas en los sistemas de información y/o sistemas de uso misional, deben ser solicitadas a través del formato GTIC-F-001 Formato Creación, modificación o eliminación de Usuarios y deberán crearse con el siguiente estándar:

- Primera letra del nombre, seguido de la segunda letra del nombre (si aplica), primer apellido y finaliza con la inicial del segundo apellido (si aplica). En caso de que exista un usuario con la definición establecida, se procede con de la segunda letra del nombre (si aplica), primer apellido y finaliza con la inicial del segundo apellido (si aplica).

  Juan Manual Gutiérrez Ramírez -> jmgutierrezr

  Juan Manual Gutiérrez Ramírez -> mgutierrezr

Las cuentas de usuario se crearán cuando el área de Gestión Humana (empleados directos) o área Administrativa y Financiera (Contratistas) realicen el reporte al área de TI sobre el ingreso, dicha solicitud debe contener todos los accesos requeridos, se debe crear un usuario único a cada colaborador.

6.4.2 Actualizar cuentas de usuario

En caso de ascenso, cambio de cargo o rol de un colaborador, el área de Gestión Humana (empleados directos) o área Administrativa y Financiera (Contratistas) deberán informar al área de TI para la suspensión de los accesos que ya no se requieran y la activación de los nuevos que apliquen.

6.4.3 Suspensión de cuentas de usuario

En caso de terminación de la relación laboral de un empleado directo o contratista con la entidad, el área de Gestión Humana (empleados directos) o área Administrativa y Financiera (Contratistas) hará el respectivo reporte al área de TI, quienes, a su vez, deberán proceder con la eliminación inmediata de todos los accesos a los sistemas de información de la Operadora Distrital de Transporte. De esta forma se garantizará que retiran y/o bloquean los derechos de acceso a los usuarios que se han retirado de la entidad.

6.4.4 Revisión de cuentas de usuario

Se debe realizar una revisión de cuentas de usuario para validar la integridad de estas y garantizar que cumple con los parámetros de seguridad establecidos. La auditoría de las cuentas de usuario se realiza de la siguiente manera:

- La revisión de políticas y configuración aplicadas (incluido contraseñas) a cuentas de usuario debería ser por reportes de consolas de configuración.

- Se debe realizar un cruce entre el personal activo en la base de datos TI versus el personal activo del área de Gestión Humana (empleados directos) o área Administrativa y Financiera (Contratistas), para garantizar que los usuarios que ya no pertenecen a la compañía no tengan cuentas activas.

6.5 Política de Contraseñas [6]

Control:	A.9.3 Responsabilidades del usuario
Objetivo:	Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, hagan uso de cualquier tipo de sistema de información relacionada con el objeto misional de la entidad.

Lineamientos:

- Se activará para todos los usuarios el doble factor de autenticación para ingreso a Office 365.
- Los usuarios deben recibir un aviso por parte de la aplicación antes de que expire la contraseña.
- Como mecanismo para mitigar el riesgo de ataques informáticos, las cuentas serán bloqueadas de cinco (5) intentos fallidos de inicio de sesión, en caso de generarse bloqueo, se debe solicitar al área de TI para que realicen el proceso necesario para el desbloqueo de la cuenta.
- Las contraseñas por omisión que vienen en los sistemas y software deben ser modificadas enseguida de su instalación.

6.5.1 Creación de contraseñas

- Toda contraseña que se asigne por primera vez o en un restablecimiento de contraseña estará denominada de primer uso y estará forzada al cambio inmediato cuando el sistema lo solicite.
- El estándar de las contraseñas deberá atender las siguientes consideraciones:
  - 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): (~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /)

[6] ISO/IEC 27001:2013 Anexo A, Ítem 9.3

- Se debe evitar el uso de información como nombres, apellidos, ciudad, entre otras que sean fácilmente deducibles.
- No se podrá utilizar secuencias ni numéricas o de caracteres básicas de teclado tales como 1234 o asdf.

6.5.2 Actualización de contraseñas

- Todas las cuentas de correo tienen activo el doble factor de autenticación, lo que potencializa la seguridad de cuentas. Sin embargo, estas serán forzadas a cambiarse cada seis (6) meses, como directriz de seguridad de la Operadora Distrital de Transporte.
- No se deben usar contraseñas repetidas, el sistema tendrá en cuenta un historial de las ultimas 4 contraseñas usadas.

6.5.3 Uso correcto de contraseñas

- Cualquier funcionario y/o contratista deberá reportar cualquier sospecha de que una persona esté utilizando credenciales de acceso o un usuario que no le pertenece, y. Por lo que se deberá informar al usuario para realizar el cambio de contraseña de inmediato o informar al área de TI.
- Siempre se deberá digitar usuario y contraseña para acceder a las diferentes aplicaciones de la ODT; 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.
- La contraseña es única e intransferible, en ningún caso se debe realizar el préstamo de esta, y por lo tanto se deberá tener precaución en su digitación para que otros funcionarios y/o contratistas o personas mal intencionadas logren accesos no autorizados a las aplicaciones de la entidad.
- Por ningún motivo los usuarios deberán marcar las casillas de recordar usuarios y contraseñas.

6.6 Política de Manejo de Software[7]

Control:	A.12.2 Protección contra el software malicioso (malware)
Objetivo:	Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, hagan uso de cualquier tipo de sistema de

[7] ISO/IEC 27001:2013 Anexo A, Ítem 12.2

información y/o herramientas informáticas relacionada con el objeto misional de la entidad.

Lineamientos:

- No está permitido copiar, generar, escribir, propagar, compilar, ejecutar o intentar introducir cualquier código de programación diseñado para dañar, auto replicarse o afectar el desempeño de cualquier equipo o red de la entidad.
- Los sistemas, equipos e información la OPERADORA DISTRITAL DE TRASNPORTE deben ser revisados periódicamente para verificar que no haya presencia de código malicioso.
- Todo software que no esté en la nube y que requiera de una ejecución propia en los portátiles o equipos de escritorio para ejercer las funciones propias del cargo, deberán contar con el respectivo licenciamiento al día.
- La instalación de cualquier tipo de software deberá ser autorizado por el área de TI o por personal que cuente con la autorización y permisos otorgados por el Formato GTIC-F-004 Formato de Solicitud Para instalación de Software.
- No será permitido el almacenamiento de material multimedia de uso personal tal como: música, videos, películas, entre otros.
- Está prohibido la instalación o descarga de software de fuentes no confiables, no autorizados o no licenciados.
- El área de TI es la encargada de instalar y mantener actualizado el software para la detención y reparación de virus, escanear computadores o medios extraíbles.

6.7 Política Equipos de Cómputo, puesto de trabajo y pantalla limpia[8]

Control:	A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia
Objetivo:	Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, hagan uso de cualquier tipo de herramientas informáticas.

Lineamientos:

- Los usuarios deben bloquear su sesión cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del usuario. Esto sin importar que tan cerca del equipo se encuentre. Para estos los usuarios podrán ejecutar (Windows + L).

[8] ISO/IEC 27001:2013 Anexo A, Ítem 11.2.8 y 11.2.9

- Los equipos de cómputo deben ser conectados a una red eléctrica regulada, para garantizar su continuidad ante posibles caídas de fluido eléctrico.
- Todos los equipos de cómputo (portátiles o de escritorio) deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la OPERADORA DISTRITAL DE TRANSPORTE, el cual se activará automáticamente después del tiempo de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.
- Los funcionarios y/o contratistas deberán retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
- Se debe guardar bajo llave, documentos impresos (en papel) o medios informáticos (USB, discos extraíbles) cuando no sea necesario su uso.

6.8 Política de uso de redes y comunicaciones electrónicas[9]

Control:	A.13 Seguridad de las comunicaciones
Objetivo:	Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, hagan uso redes o comunicaciones electrónicas de la entidad.

Lineamientos:

- Los canales de comunicación de la OPERADORA DISTRITAL DE TRASNPORTE son de uso exclusivo para ejecutar cada una de las funciones del cargo asignado. Por lo que no podrán ser utilizados para temas personales.
- No se podrá hacer uso del correo electrónico u otros medios de comunicación para el envío de contenido de tipo ilegal o fraudulento.
- Está prohibido hacer uso de las redes o herramientas tecnológicas para consulta de sitios con contenido pornográfico, violento o que atente con la integridad, sexualidad o discapacidad de otras personas.
- Las cadenas de información que no tengan relación con temas misionales de la entidad están totalmente prohibidas.
- Las redes sociales o mensajería instantánea deberán estar enmarcado en un vocabulario cordial, amable y respetuoso. No se deberá crear polémicas y tampoco tratar temas de índole político, religioso, sexual o descalificativo.
- Todos los sistemas de la OPERADORA DISTRITAL DE TRANSPORTE sean propios o subcontratados, y en los que se genere o se procese cualquier tipo de información, son de uso exclusivo para ejecutar las funciones propias del cargo, pero

[9] ISO/IEC 27001:2013 Anexo A, Ítem 13

de propiedad de la entidad, por lo que no se podrá compartir o negociar con los mismos.

6.9 Política de seguridad física[10]

Control:	A.11 Seguridad física y del entorno
Objetivo:	Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.
Alcance:	La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes. o que, por su rol, tengan acceso a la entidad.

Lineamientos:

6.9.1 Áreas Físicas

- Se cuenta con una empresa de seguridad encargada de velar por las instalaciones del patio al igual que el monitoreo de las cámaras. De igual manera se tiene la entrada principal con registro dactilar para funcionarios y contratistas.
- Se debe contar con cámaras de seguridad en las áreas donde se encuentre instalados los centros de procesamiento de información, suministro de energía eléctrica, o cualquier otra área considerada critica para el correcto funcionamiento misional de la entidad.

6.9.2 Condiciones Generales de Ingreso de funcionarios, contratistas y/o visitantes

- Para el personal de planta y contratistas de la ODT de la Operadora La Rolita el ingreso se realizará con control biométrico y el carné institucional.
- Para visitantes o contratistas externos, las Gerencias y/o dependencias deben enviar un día antes el pago de seguridad social completo (ARL, EPS y Pensión) y el formato “Registro de Ingreso Personal” diligenciado, al área SST y Administrativa informando la labor a realizar.
- La información se debe enviar a los siguientes correos: emgomezm@odt.gov.co y rriosp@odt.gov.co, a más tardar a las 3:00 p.m.
- Para el ingreso a las áreas de mantenimiento y operación es obligatorio el uso de calzado de seguridad.
- Si se realiza trabajo en alturas o tareas de alto riesgo, adicionalmente se deben enviar los siguientes documentos:

[10] ISO/IEC 27001:2013 Anexo A, Ítem 11

- Certificado de entrenamiento avanzado.
- Certificado del coordinador que diligenciará los permisos de trabajo.

- Si el ingreso se realiza con vehículo particular, se debe incluir en el correo de solitud la placa del vehículo y esta se encuentra sujeto a previa verificación de disponibilidad de cupos.
- Si el ingreso se realiza con vehículo de carga, se debe incluir en el correo de solitud la placa del vehículo, descripción de los materiales a ingresar o recoger, y de la zona de cargue o Descargue.

6.9.3 Normas generales de seguridad en el patio

- Todo contratista o visitante debe presentar su cédula al guarda de seguridad, de lo contrario no se le permitirá el ingreso.
- Todo contratista o visitante sin excepción, deberá realizar el registro correspondiente antes de ingresar a las instalaciones de nuestra Entidad.
- Se debe transitar únicamente por las zonas peatonales autorizadas, sin correr.
- El límite de velocidad permitido es de 10 km/h para tránsito vehicular dentro de las instalaciones; los vehículos particulares deberán ingresar con las luces de parqueo encendidas en todo momento.
- Se debe realizar el PARE en los pasos peatonales dando prioridad al peatón.
- No está permitido el uso de equipos celulares en vías de circulación del patio.
- No está permitido el consumo de alimentos en las áreas de trabajo y/o zonas de parqueo.
- Se prohíbe el ingreso en estado de embriaguez o bajo efectos de sustancias psicoactivas.
- Prohibido fumar al interior de estas instalaciones.
- Se debe transitar por las escaleras con precaución e identificar las salidas de emergencia y los puntos de encuentro.
- En caso de emergencia siga las instrucciones de los brigadistas
- No podrá ingresar a los lugares de trabajo sin ser autorizado.
- Se deben reportar las condiciones y actos inseguros.
- No obstaculizar los equipos y elementos de emergencia.
- No obstaculizar lo pasos peatonales, pasillos, escaleras o puertas.
- Mantener las áreas de trabajo, de descanso, casino y baños, limpias y organizadas.
- Hacer uso sostenible y consumo consiente de los recursos de agua y luz.

- Todo contratista será responsable de los residuos generados durante las actividades, por lo tanto, se hará cargo de la disposición final de estos, no se almacenarán en el patio.
- Al almacenar material de obra como arenas y gravas, este deberá estar cubierto, evitando contaminación atmosférica.
- Se prohíbe el uso de dispositivos sonoros, mantener la voz baja.
- Hacemos parte de una comunidad y debemos tener convivencia responsable con nuestros vecinos. No generar ninguna acción que falte a esta norma.

6.9.4 Equipos de protección y condiciones de seguridad en lugares de trabajo

- Es obligatorio el uso adecuado de equipos, elementos de protección personal y dotación definidos para las actividades a realizar.
- Use careta de seguridad en tareas con riesgo de proyección de partículas, líquidos y objetos en la cara.
- Use guantes de seguridad en tareas con riesgo de cortes, raspaduras, machucones y manipulación de químicos.
- Use calzado de seguridad acorde a la labor.
- • No use joyería ni otro elemento que genere riesgo de atrapamiento.
- • Para pruebas de frenado y potencia que requieran exceder el límite de 10 Km/h, se debe
- señalizar la zona.
- Para labores nocturnas, se debe hacer uso de prendas reflectivas.
- Para transito nocturno de vehículos en el patio, siempre encender las luces.
- Para trabajos nocturnos dentro de un bus (mantenimiento, limpieza, alistamiento, etc.) siempre encender la iluminación interna de los vehículos.
- Evite transitar por puntos ciegos para los vehículos en las zonas de mantenimiento y parqueo (efecto cortina).
- Todo contratista deberá contar con su kit de derrames, en caso de presentarse un derrame deberá atenderlo e informar a la ODT de manera inmediata.
- Notifique los daños o mal funcionamiento de la infraestructura, herramientas, maquinaria o equipos.

6.9.5 Suministros

- Todos los equipos críticos deben estar protegidos ante posibles fallas de suministro de energía.
- Se deberá contar con UPS y/o plantas eléctricas, las cuales deberán ser revisadas periódicamente para asegurar su correcto funcionamiento, esta labor deberá ser realizada por personal idóneo.

6.9.6 Cableado

- El cableado eléctrico debe cumplir con los requisitos técnicos aplicables a las normas vigentes.
- Se debe evitar la interferencia entre el cableado eléctrico y de datos.
- El cableado de red se debe proteger contra daños o intervención de personal no autorizado.

6.10 Política de Gestión Humana[11]

Control: A.7 Seguridad relativa a los recursos humanos

Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

Alcance: La presente política aplica para todos funcionarios y/o contratistas, que vayan a desempeñar cargos dentro de la entidad.

Lineamientos:

- Se deben realizar las validaciones correspondientes a los candidatos a ocupar algún cargo en la entidad antes de su contratación, como son la validación de antecedentes disciplinarios, referencias académicas, laborales y todas las que se consideren desde el área de Recursos Humanos.
- Se deberá firmar un acuerdo de confidencialidad en el momento de su contratación, donde se acepte las políticas de seguridad vigentes de la entidad.
- Se deberá reportar de manera inmediata la desvinculación o novedades de los funcionarios para ejecutar los procedimientos correspondientes de manera temporal (vacaciones, licencias, incapacidades) o definitivas (desvinculación) con el fin de garantizar la confidencialidad de la información de la entidad.
- Cuando se presente una desvinculación se deberán entregar todos los activos entregados al iniciar labores o durante la ejecución de su cargo.

[11] ISO/IEC 27001:2013 Anexo A, Ítem 7

6.11 Política de tratamiento de Datos Personales[12]

Control: A.18.1.4 Protección y privacidad de la información de carácter personal

Objetivo: Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables

Alcance: La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes.

Lineamientos:

- Por medio de la ley 1581 de 2012 se reglamenta el tratamiento de datos personales en Colombia, porque la OPERADORA DISTRITAL DE TRANSPORTE da cumplimiento mediante el documento de Política de protección de datos personales.

6.12 Cumplimiento[13]

Control: A.18.Cumplimiento

Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

Alcance: La presente política aplica para todos funcionarios, contratistas, proveedores, y terceras partes.

Lineamientos:

- Los gerentes o responsables de los procesos deberán velar por la correcta implementación y cumplimiento de las normas, políticas y procedimientos de seguridad de la información en sus áreas de responsabilidad. Cualquier incumplimiento se actuará con lo establecido en el reglamento interno de la entidad.
- Se realizarán validaciones periódicas de los sistemas de información con el fin de verificar el cumplimiento de los lineamientos de la entidad.
- Los gerentes o responsables de los procesos deberán velar por el cumplimiento de los requisitos contractuales adquiridos con terceros según correspondan.

[12] ISO/IEC 27001:2013 Anexo A, Ítem 18.1.4
[13] ISO/IEC 27001:2013 Anexo A, Ítem 18