POLÍTICA DE SEGURIDAD DIGITAL

2023

TERMINAL METROPOLITANA
de Transportes de Barranquilla S.A.

TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA

POLÍTICA DE SEGURIDAD DIGITAL

TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA S.A.

SUBGERENCIA DE PLANEACIÓN, PROYECTOS, DESARROLLO Y TICS

OFICINA DE SISTEMAS

AÑO 2023

Carrera 14 # 54 - 186 Módulo D 1er piso . Tel (57) 605 393 00 43
www.ttbaq.com.co . ventanillaunicaderadicacion@ttbaq.com.co
Nit 890.106.084-4 . Soledad - Atlántico

1. PRESENTACIÓN

La Política de Seguridad Digital de la Terminal Metropolitana de Transportes de Barranquilla S.A. es un marco integral diseñado para proteger y salvaguardar la información digital y los sistemas de información de la empresa. Esta política tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de la información, así como prevenir y mitigar los riesgos asociados con la seguridad digital.

Esta política se aplica a todos los empleados, contratistas, proveedores y cualquier otra persona que tenga acceso a los sistemas de información de la Terminal Metropolitana de Transportes de Barranquilla S.A. Todos los usuarios de estos sistemas están obligados a cumplir con esta política y a participar activamente en la protección de los activos de información de la empresa.

La política de seguridad digital se basa en las mejores prácticas de la industria y cumple con todas las leyes y regulaciones locales relevantes, incluyendo pero no limitado al Acuerdo 08 de 2019, la Ley 1928 de 2018, el Acuerdo 02 de 2018, el Conpes 3854 de 2016, el Decreto 1078 de 2015, la Ley 1712 de 2014, la Ley estatutaria 1581 del 2012, el Decreto 103 de 2015 y la Ley 1273 de 2009.

La empresa se compromete a revisar y actualizar regularmente esta política para adaptarse a los cambios en el entorno de seguridad digital y para garantizar que sigue siendo efectiva y relevante.

La Terminal Metropolitana de Transportes de Barranquilla S.A. reconoce que la seguridad digital es una responsabilidad compartida y requiere el compromiso y la cooperación de todos los usuarios de los sistemas de información. Juntos, podemos trabajar para proteger la información digital de la empresa y garantizar un entorno digital seguro y confiable.

2 ANTECEDENTES

2.1 DIMENSIONES DE LA POLÍTICA DE SEGURIDAD DIGITAL

Con el fin de adoptar un enfoque multidimensional, que garantice la seguridad digital, se definen cinco dimensiones estratégicas las cuales determinan los campos de acción de la política nacional de seguridad digital.

Gobernanza de la seguridad digital: articulación y armonización de las múltiples partes interesadas, bajo un marco institucional adecuado, con el fin de gestionar la seguridad digital, bajo el liderazgo del Gobierno nacional.

Marco legal y regulatorio de la seguridad digital: marco legal y regulatorio que soporta todos los aspectos necesarios para adelantar la política.

Gestión sistemática y cíclica del riesgo de seguridad digital: conjunto de iniciativas, procedimientos o metodologías coordinadas con el fin de abordar, de manera cíclica y holística, los riesgos de seguridad digital en el país.

Cultura ciudadana para la seguridad digital: sensibilización de las múltiples partes interesadas, para crear y fomentar una cultura ciudadana responsable en la seguridad digital.

Capacidades para la gestión del riesgo de seguridad digital: fortalecimiento y construcción de capacidades humanas, técnicas, tecnológicas, operacionales y administrativas en las múltiples partes interesadas, para adelantar la gestión de riesgos de la seguridad digital.

2.2 ESTRATEGIA DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La estrategia de gestión de riesgos para abordar la seguridad digital debe tener un enfoque flexible y ágil para abordar las incertidumbres digitales. Lo anterior, con el fin de alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales, y proteger a las personas frente a las amenazas de seguridad digital.

De acuerdo con las recomendaciones de la OCDE, la estrategia nacional debe ser consistente con el conjunto de principios formulados, debe crear las condiciones para que las múltiples partes interesadas puedan gestionar la seguridad digital de sus actividades, debe fomentar la confianza en el entorno digital y, además, debe:

- Estar apoyada desde el más alto nivel;
- Definir claramente que su objetivo es aprovechar el entorno digital abierto;
- Debe ser el resultado de un enfoque coordinado, abierto y transparente, donde participen las partes interesadas.

La política de seguridad digital de la Terminal Metropolitana de Transportes de Barranquilla se basa en unos principios fundamentales, que contemplan:

- Salvaguardar los derechos humanos y los valores fundamentales de los interesados.
- Adoptar un enfoque incluyente y colaborativo que involucre activamente a todos los interesados.
- Asegurar una responsabilidad compartida entre todos los actores involucrados.
- Adoptar un enfoque basado en riesgos, que permita a los individuos el libre, confiable y seguro desarrollo de sus actividades en el entorno digital.

2.3 ALCANCE

La presente política se aplica a todos los usuarios, empleados, contratistas, proveedores y cualquier otra persona que tenga acceso a los sistemas de información de la Terminal Metropolitana de Transportes de Barranquilla S.A.

2.4 MARCO LEGAL

MARCO NORMATIVO	DESCRIPCIÓN
Decreto 1151 de 2008	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente

	la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Conpes 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016	El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo

	nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
Conpes 3975	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
Circular 018 de 2021	Implementación de la resolución 1519 de 2020.

2.5 Glosario

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Ataque cibernético: Acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio.

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con fin de proteger a los usuarios y los activos de la organización.

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

Incidente digital: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Riesgo de seguridad digital: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital.

Seguridad de la información: Entendida como el conjunto de elementos interrelacionados o interactuantes 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, con miras a preservar la confidencialidad, integridad, y disponibilidad de la información.

Seguridad informática: Comprende los métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información contenida en formato digital en estos medios.

Seguridad digital o ciberseguridad: Conjunto de medidas de “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”. A diferencia de la seguridad de la información, en la ciberseguridad se aplican medidas ofensivas y no solo de defensa.

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

3. POLÍTICA

La Terminal Metropolitana de Transportes de Barranquilla S.A. desarrollará la gestión de los riesgos de seguridad digital, de conformidad con los lineamientos establecidos en la Guía para la gestión de riesgos de seguridad digital para el sector mixto y privado, la cual tiene como objetivo orientar a las organizaciones del sector privado y mixto en el desarrollo de la metodología para la gestión de riesgos de seguridad digital (GRSD), enmarcadas en un ciclo Deming o PHVA.

Para cada una de las fases de la gestión del riesgo digital, es necesario tener en cuenta la comunicación y la consulta y los principios fundamentales y generales, con el fin de crear las condiciones para que las múltiples partes interesadas y la ciudadanía en general puedan gestionar los riesgos de Seguridad Digital de sus actividades económicas y sociales, fomentando la confianza en el entorno digital.

ALCANCE

Para el cumplimiento de la presente Política de Seguridad Digital se define el siguiente alcance:

1. La Oficina de Sistemas, la Secretaría General por medio de la Oficina de de Atención al Ciudadano y Gestión Documental, revisarán y actualizarán los activos de información.

2. La Oficina de Sistemas hará el levantamiento de la Infraestructura Tecnológica crítica de la entidad.

3. La Oficina de Sistemas, apoyará la actualización de los riesgos de seguridad digital, siguiendo la metodología dispuesta por el DAFP y el Ministerio de TIC.

4. Todas las dependencias con el apoyo de la Subgerencia de Planeación, Proyectos, Desarrollo y TICs implementarán el Modelo de Seguridad y Privacidad de la Información MSPI con las herramientas que el Ministerio de TIC destine para ello, el cual integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad digital.

6. La Subgerencia de Planeación, Proyectos, Desarrollo y TICs, evaluarán el desempeño del Modelo de Seguridad y Privacidad de la Información MSPI, a través de la aplicación de la Política de Seguridad y Privacidad de la Información, la ejecución de los controles definidos en la declaración de aplicabilidad y el monitoreo de los indicadores de seguridad de la información.

7. La Subgerencia de Planeación, Proyectos, Desarrollo y TICs, sensibilizarán a usuarios internos en el uso de medios digitales y en buenas prácticas para mitigar los riesgos de seguridad digital que puedan afectar a la entidad.

SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA

La Terminal Metropolitana de Transportes de Barranquilla S.A. realizará seguimiento a través de las tres líneas de defensa definidas en el MIPG en la dimensión 7, Control Interno mediante el componente de actividades de control.

La entidad realizará seguimiento al avance de la Política, a través de la definición de indicadores en el plan de tratamiento de riesgos y seguridad de la Información.

Se realizará el seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, con la herramienta dispuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones.

La medición de la Política se realizará a través del reporte de la herramienta en línea dispuesta por el DAFP (FURAG).

POLÍTICAS PARTICULARES DE SEGURIDAD DIGITAL

El servicio de acceso a internet, intranet, sistemas de información, medios de almacenamiento, aplicaciones (software), cuentas de red, y equipos de cómputo y en general todo dispositivo tangible o intangible que tenga relación directa o indirecta con las tecnologías de la información y las comunicaciones TIC, son propiedad de la Terminal Metropolitana de Transportes de Barranquilla S.A. y deben ser usados únicamente para el cumplimiento de las funciones misionales asignadas a los servidores públicos y/o contratistas de la entidad.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales excepto de las autorizadas por los secretarios o directores de despacho, asumiendo así la responsabilidad de posibles fugas de información por éstos.

USO DE CORREO CORATIVO

- La cuenta de correo electrónico y la clave asociada asignada es personal, intransferible y por razones de seguridad deberá ser cambiada periódicamente.

- La cuenta de correo es de uso exclusivo para cumplir las funciones misionales del servidor público al cual fue asignada, no deberá usarse para otros fines.

- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera exclusiva a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

- El usuario será responsable de revisar y depurar su buzón de correo periódicamente, a fin de evitar que éste se sature.

- Cuando un servidor público tiene asignada una cuenta de correo de la entidad, y se desvincula, deberá entregar a la Oficina de Sistemas los usuarios y password asignados, de igual manera dicha información debe entregarse cuando exista un proceso de empalme.

POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

Para lograr un alto rendimiento y salvaguarda de computadores y portátiles, la se han definido los siguientes parámetros:

- Los computadores de mesa, portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la aprobación del jefe de la dependencia que lo tiene asignado.

- El equipo de cómputo asignado deberá ser para uso exclusivo del servidor público para el ejercicio de las funciones asignadas.

- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.

- Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información

sensible que se encuentre en el equipo, previniendo así la pérdida involuntaria de información, derivada del proceso de reparación.

- Debe respetarse y no modificar la configuración de hardware y software establecida por la Oficina de Sistemas.

- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón, es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a la Oficina de Sistemas.

- No debe utilizarse software descargado de internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado de forma rigurosa y que esté aprobado su uso por Oficina de Sistemas.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio servidor público.

- La Oficina de Sistemas no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y/o manejo de información) a equipos que no sean de la Entidad.

- Se prohíben que los equipos (computador y/o portátil) estén en contacto con piso, el usuario debe disponerlos sobre el escritorio.

CONTROL DE ACCESO

Tener en cuenta la Política de Control de Acceso definida.

ADMINISTRACIÓN DE USUARIOS

Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que deben ser únicos por cada servidor público o tercero.

Cuando se retire o cambie de contrato cualquier servidor público o tercero, se deberá aplicar la eliminación o cambios de privilegios en los sistemas de información a los que el usuario estaba autorizado.

La Oficina de Sistemas deberá realizar periódicamente revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los servidores públicos y/o contratistas.

Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

Si los sistemas de información detectan inactividad por un periodo igual o superior a diez minutos, deben automáticamente aplicar “time out”, es decir, finalizar la sesión de usuario.

POLÍTICAS DE ACCESO A INTERNET

Los servicios de correo electrónico e internet, son administrados por la Subgerencia de Planeación, Proyectos, Desarrollo y TICs, la cual monitoreará las actividades de la red, tanto para correo electrónico, internet y uso de red de datos con el fin de vigilar el cumplimiento de las políticas establecidas para el uso de tecnologías de la información.

- No se podrá utilizar el internet como un medio de participación, acceso y distribución de actividades o materiales que vayan en contra de la Ley.

- La Subgerencia de Planeación, Proyectos, Desarrollo y TICs asignará a cada usuario, permisos y perfiles de navegación dependiendo de las actividades que realice.