INFORME DE SEGUIMIENTO A LA POLITICA DE SEGURIDAD DIGITAL RESOLUCION N° 036 DE 31 DE ENERO DE 2023

OFICINA DE CONTROL INTERNO

TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA
NOVIEMBRE 2024

INTRODUCCION

Las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas deben implementar la Política de Gobierno Digital en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política y Art. 2.2.9.1.1.2. Decreto 1078 de 2015.

Así mismo, la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital, ha sido desarrollado y socializado por Ministerio de las Tecnologías de la Información y comunicaciones), por parte departamentos administrativos de la rama ejecutiva a las entidades territoriales.

Dentro de las recomendaciones dadas por el Ministerio de las Tecnologías de la información y comunicaciones a las entidades territoriales tenemos las siguientes:

- ✓ Fortalecer las capacidades en seguridad digital de la entidad a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital

- ✓ Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar.

- ✓ Realizar periódicamente ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos

- ✓ Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética.

- ✓ Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.

- ✓ Fortalecer las capacidades en seguridad digital de la entidad a través de ejercicios de simulación de incidentes de seguridad digital al interior de la entidad

OBJETIVO

Con este informe la oficina de Control interno verifica y evalúa el cumplimiento de la política de Seguridad Digital de conformidad los lineamientos establecidos por el gobierno nacional (Ministerio de tecnologías de la información y comunicaciones,), teniendo en cuenta las dimensiones de la seguridad digital y la estrategia de gestión de riesgos adoptada en la entidad.

Así mismo, se realiza la verificación de las acciones que conlleven al cumplimiento de los lineamientos establecidos para la política de Seguridad de la Información y Protección de Datos Personales para la vigencia 2024.

ALCANCE

Verificar la implementación los lineamientos y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información en el ámbito del gobierno digital, así como, para proteger los datos personales conforme a la legislación vigente. Esto incluye la identificación de riesgos, implementación de controles y capacitación del personal para promover una cultura de seguridad de la información vigencia 2023.

NORMATIVIDAD

- ✓ Decreto 767 de 2022 “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”
- ✓ Acuerdo 08 de 2019
- ✓ Ley 1928 de 2018 “Por medio de la cual se aprueba el "convenio sobre la. ciberdelincuencia",
- ✓ Decreto 1008 del 14 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

- ✓ Acuerdo 02 de 2018
- ✓ Conpes 3854 de 2016
- ✓ 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”
- ✓ Ley 1712 de 2014 -Transparencia y Acceso a la Información Pública
- ✓ Ley 1581 de 2012. Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
- ✓ Decreto 2573 de 2014. “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea”, Artículo No. 5. Componentes.
- ✓ 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”
- ✓ Autodiagnóstico de gestión de Política de Gobierno Digital MIPG.

METODOLOGIA

La Oficina de Control Interno con el fin de evaluar el cumplimiento de los lineamientos establecidos en la estrategia de Gobierno Digital, mediante correo electrónico del día 14 de noviembre de 2024 informó y solicitó la información relacionada con el autodiagnóstico de la política de gobierno y seguridad digital, la adopción de las políticas de seguridad digital y los resultados de la medición del índice de desempeño (FURAG) de la política de seguridad digital vigencia 2023; Así mismo, la información referente a la política de seguridad de información y protección de datos personales vigente, según el Decreto 1078 de 2015.

AUTODIAGNÓSTICO DE GOBIERNO DIGITAL

Se evidencia la realización del autodiagnóstico de Gobierno digital para la vigencia 2024, de conformidad con la información suministrada por la oficina de sistemas.

A continuación, se muestra el resultado obtenido en el autodiagnóstico:

El futuro digital es de todos | MinTIC

mipg modelo integrado de planeación y gestión

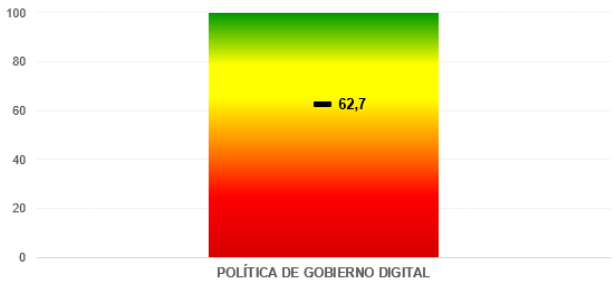
AUTODIAGNÓSTICO POLÍTICA DE GOBIERNO DIGITAL

ENTIDAD	CALIFICACIÓN TOTAL
	62,7

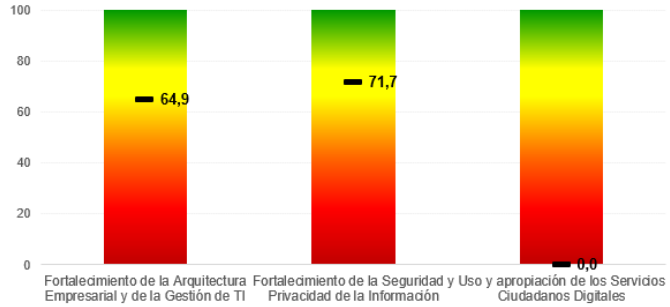
HABILITADORES / PROPÓSITOS	CALIFICACIÓN	ÍTEM	PORCENTAJE DE CUMPLIMIENTO	OBSERVACIONES
Fortalecimiento de la Arquitectura Empresarial y de la Gestión de TI	64,9	Con respecto al Plan Estratégico de Tecnologías de la Información (PETI) para esta vigencia, la entidad: -Lo formuló, está aprobado y se ha integrado al plan de acción anual	100	
		El Plan Estratégico de Tecnologías de la Información (PETI) incluye: A. El portafolio o mapa de ruta de los proyectos	NA	
		El Plan Estratégico de Tecnologías de la Información (PETI) incluye: B. La proyección del presupuesto	100	
		El Plan Estratégico de Tecnologías de la Información (PETI) incluye: C. El entendimiento estratégico	100	
		El Plan Estratégico de Tecnologías de la Información (PETI) incluye: D. El análisis de la situación actual	100	
		El Plan Estratégico de Tecnologías de la Información (PETI) incluye: E. El plan de comunicaciones del PETI	100	
		El Plan Estratégico de Tecnologías de la Información (PETI) incluye: F. Tablero de indicadores para el seguimiento y control	100	
		El Plan Estratégico de Tecnologías de la Información (PETI) incluye: G. Definición de la situación objetivo y modelo de gestión de TI	100	
		Para la gestión de tecnologías de la información (TI), la entidad cuenta con: A. Un esquema de soporte con niveles de atención (primer, segundo y tercer nivel) a través de un punto único de contacto y soportado por una herramienta tecnológica, tipo mesa de servicio que incluya al menos la gestión de problemas, incidentes, requerimientos, cambios, disponibilidad y conocimiento	100	
		Para la gestión de tecnologías de la información (TI), la entidad cuenta con: B. Un proceso para atender los incidentes y requerimientos de soporte de los servicios de TI, tipo mesa de ayuda	70	

RESULTADOS AUTODIAGNÓSTICO POLÍTICA DE GOBIERNO DIGITAL

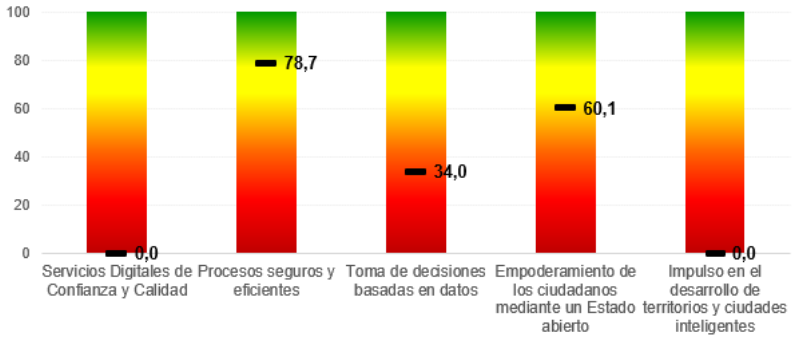
1. Calificación total:



2. Calificación de los habilitadores de la Política de Gobierno Digital:



3. Calificación de los propósitos de la Política de Gobierno Digital:



Se evidencia plan de accion de la oficina de sistemas, en donde se evidencian las siguientes actividades:

POLITICAS MIPG	DESCRIPCIÓN DE LA ACCIÓN	ACTIVIDADES	INDICADORES	METAS	RESPONSABLES
SEGURIDAD DIGITAL	Sensibilización a funcionarios y contratistas	Enviar mensajes al de sensibilización al correo y a través de WhatsApp a los funcionarios con relación a las políticas de seguridad de la información y protección de datos personales y de control de acceso a equipos (dos al año)	# de actividades realizadas / # de actividades programadas	Realizar una jornada de sensibilización	JEFE OFICINA DE SISTEMAS
	Realización de Backups	Realizar copias de seguridad de la información	# Copias de seguridad programadas / # Copias realizadas	Realizar el 100% de las copias de seguridad programadas	JEFE OFICINA DE SISTEMAS
GOBIERNO DIGITAL	Formulación y aprobación del PETI	Formular el PETI y presentar para su aprobación	PETI aprobado	Aprobar el PETI	JEFE OFICINA DE SISTEMAS
		Publicar el PETI en la página web	PETI publicado en la página web	Publicar el PETI	JEFE OFICINA DE SISTEMAS
	Elaboración del esquema de soporte	Elaborar el esquema de soporte para atención a requerimientos	Esquema de soporte elaborado	Elaborar y dar a conocer el esquema de soporte	JEFE OFICINA DE SISTEMAS
	Catálogo de servicios de TI	Elaborar el catálogo de servicios de TI	Catálogo de Servicios de TI elaborado	Elaborar el catálogo de servicios de TI	JEFE OFICINA DE SISTEMAS
	Catálogo de Sistemas de Información	Elaborar el catálogo de Sistemas de Información	Catálogo de Sistemas de Información elaborado	Elaborar el catálogo de Sistemas de Información	JEFE OFICINA DE SISTEMAS
	Programa de Disposición final de Residuos Tecnológicos	Elaborar el Programa de Correcta Disposición final de Residuos Tecnológicos	Programa Correcta Disposición final de Residuos Tecnológicos	Elaborar el Programa Correcta Disposición final de Residuos Tecnológicos	JEFE OFICINA DE SISTEMAS
	Mantenimiento preventivo de equipos	Elaborar el plan de mantenimiento preventivo de equipos de cómputo e impresoras	# de planes proyectados / # de planes elaborados	Elaborar el plan de mantenimiento	JEFE OFICINA DE SISTEMAS
		Elaborar el cronograma de mantenimiento de equipos	Cronograma de mantenimiento elaborado	Elaborar el cronograma de mantenimiento de equipos	PROFESIONAL UNIVERSITARIO DE SISTEMAS
		Realizar los mantenimientos de acuerdo con lo estipulado en el cronograma	# Mantenimientos programados / Mantenimientos realizados	Realizar el 100% de los mantenimientos programados	PROFESIONAL UNIVERSITARIO DE SISTEMAS
	Soporte tecnológico	Documentar el procedimiento de Soporte Tecnológico	Procedimiento de soporte tecnológico elaborado	Documentar el procedimiento de Soporte Tecnológico	JEFE OFICINA DE SISTEMAS
		Atender las solicitudes de soporte generadas en las dependencias	# Soportes realizados / # Solicitudes de Soporte	Atender el 100% de las solicitudes de soporte	JEFE OFICINA DE SISTEMAS / P U SISTEMAS

A la fecha de septiembre 2024 (Tercer seguimiento del plan de accion), encontramos el siguiente avance de las actividades establecidas:

POLITICAS MIPG	DESCRIPCIÓN DE LA ACCIÓN	ACTIVIDADES	INDICADORES	METAS	AVANCE A SEPT 2024
SEGURIDAD DIGITAL	Sensibilización a funcionarios y contratistas	Enviar mensajes al de sensibilización al correo y a través de WhatsApp a los funcionarios con relación a las políticas de seguridad de la información y protección de datos personales y de control de acceso a equipos (dos al año)	# de actividades realizadas / # de actividades programadas	Realizar una jornada de sensibilización	100% Se realizo y se compartió por el grupo de WhatsApp institucional
	Realización de Backups	Realizar copias de seguridad de la información	# Copias de seguridad programadas / # Copias realizadas	Realizar el 100% de las copias de seguridad programadas	75% Se viene realizando las copias de seguridad programadas en los servidores generadas como tareas automáticas diarias del sistema
GOBIERNO DIGITAL	Formulación y aprobación del PETI	Formular el PETI y presentar para su aprobación	PETI aprobado	Aprobar el PETI	100% Se encuentra aprobado por el Comité Institucional de gestión y desempeño para la vigencia 2024
		Publicar el PETI en la página web	PETI publicado en la página web	Publicar el PETI	100% Se encuentra publicado en la página web de la entidad en el enlace: https://www.ttbaq.com.co/planeación/
	Elaboración del esquema de soporte	Elaborar el esquema de soporte para atención a requerimientos	Esquema de soporte elaborado	Elaborar y dar a conocer el esquema de soporte	100% Esquema de publicación elaborado y publicado en la página web https://www.ttbaq.com.co/Datos%20abiertos/
	Catálogo de servicios de TI	Elaborar el catálogo de servicios de TI	Catálogo de Servicios de TI elaborado	Elaborar el catálogo de servicios de TI	75% Se encuentra en construcción
	Catálogo de Sistemas de Información	Elaborar el catálogo de Sistemas de Información	Catálogo de Sistemas de Información elaborado	Elaborar el catálogo de Sistemas de Información	75% Se encuentra en construcción
	Programa de Disposición final de Residuos Tecnológicos	Elaborar el Programa de Correcta Disposición final de Residuos Tecnológicos	Programa Correcta Disposición final de Residuos Tecnológicos	Elaborar el Programa Correcta Disposición final de Residuos Tecnológicos	100% se encuentra elaborado

POLITICAS MIPG	DESCRIPCIÓN DE LA ACCIÓN	ACTIVIDADES	INDICADORES	METAS	AVANCE A SEPT 2024
GOBIERNO DIGITAL	Mantenimiento preventivo de equipos	Elaborar el plan de mantenimiento preventivo de equipos de cómputo e impresoras	# de planes proyectados / # de planes elaborados	Elaborar el plan de mantenimiento	100% El plan de mantenimiento se encuentra elaborado
		Elaborar el cronograma de mantenimiento de equipos	Cronograma de mantenimiento elaborado	Elaborar el cronograma de mantenimiento de equipos	100% El cronograma de mantenimiento se encuentra elaborado
		Realizar los mantenimientos de acuerdo con lo estipulado en el cronograma	# Mantenimientos programados / Mantenimientos realizados	Realizar el 100% de los mantenimientos programados	75% Se están realizando los mantenimientos programados
	Soporte tecnológico	Documentar el procedimiento de Soporte Tecnológico	Procedimiento de soporte tecnológico elaborado	Documentar el procedimiento de Soporte Tecnológico	25% Este procedimiento de soporte tecnológico se encuentra en construcción
		Atender las solicitudes de soporte generadas en las dependencias	# Soportes realizados / # Solicitudes de Soporte	Atender el 100% de las solicitudes de soporte	75% A septiembre 2024, se recibieron 103 solicitudes de soporte las cuales se atendieron en su totalidad por la oficina de sistemas

PLAN ESTRATÉGICO DE TECNOLOGIAS DE LA INFORMACIÓN (PETI)

Se evidencia la elaboración y aprobación del PETI (Plan Estratégico de Tecnología de Información), mediante acta N° 1 de enero 29 de 2024 del Comité institucional de gestión y Desempeño, cumpliendo con lo establecido *en el Decreto 415 de 2016 art 2.2.35.3 Objetivos del fortalecimiento institucional y el Decreto 1078 de 2015 Art 2.2.5.1.2.2 Instrumentos- Marco de Referencia de Arquitectura Empresarial para la gestión de las TI (Tecnologías de Información) LI.ES.05. Documentación de la estrategia de TI en el PETI*.

Según la estructura del PETI este debe contener objetivo, alcance, marco normativo, análisis de la situación actual, rupturas estratégicas, entendimiento estratégico, modelo de gestión y modelo de planeación. El PETI aprobado en la Entidad contiene: objetivos, alcance, marco normativo, Alineación estratégica, Estrategias de TI (Servicios de TI, Políticas de TI, Modelo de Gobierno de TI, Modelo de gestión de TI, Estructura y

organización de TI, roles y responsabilidades de TI), Gestión de Proyectos, Gestión de información (planeación y gobierno de la gestión de la información, Dominio de arquitectura de información, Dominio de arquitectura de sistemas de información, dominio de infraestructura Tecnológica, dominio de arquitectura de seguridad, Gobierno TI, Infraestructura TI, uso y apropiación), Portafolio de iniciativas o proyectos.

Se evidencia su publicación en la página web de la entidad, según el enlace: https://www.ttbaq.com.co/wp-content/uploads/2024/02/4.3.3%20PLAN%20ESTRATEGICO-DE-TI-2024.pdf

Dentro de las actividades establecidas en el PETI encontramos:

ALINEACIÓN DE TI CON LOS PROCESOS

- Administración de cuentas de correo
- Administración de roles y perfiles usuarios
- Administración de usuarios de dominio
- Help Desk mediante la línea celular, WhatsApp y correo electrónico
- Administración del sitio Web
- Servicio de Internet
- Telefonía IP
- Conexión Wifi
- Realización backups

SERVICIOS DE TI

- Acceso a internet por Wifi
- Acceso a la red interna por VPN
- Correo electrónico y herramientas colaborativas
- Servicio de entrenamiento y capacitación uso de las soluciones de TI
- Telefonía IP
- Plataforma de Mesa de servicio
- Gestión de red de Infraestructura tecnológica
- Antivirus
- Gestión de equipos de cómputo
- Instalación de software de equipos de computo
- Página web institucional
- Soportes aplicativos
- Adquisición de licencias de software
- Mantenimiento de aplicaciones

- Administración de bases de datos
- Gestión de Backup
- Gestión de proyectos de Tecnologías de Información
- Servicio de supervisión de proveedores de TI

POLITICAS Y ESTANDARES PARA LA GESTIÓN DE LA GOBERNABILIDAD DE TI

- Gobierno digital
- Control de acceso a equipos
- Seguridad digital
- Tratamiento de riesgos y seguridad de la información
- Política de derechos de autor

POLITICA DE SEGURIDAD DIGITAL

La política de Gobierno Digital fue establecida por el gobierno nacional mediante el Decreto 1008 de 2018 (disposiciones compiladas en el Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC", capítulo 1, título 9, parte 2, libro 2), como parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de gestión para el resultado con valores, que busca promover una adecuada gestión interna de las entidades y un buen relacionamiento con el ciudadano, a través de la participación y la prestación de servicios de calidad.

Es importante tener en cuenta, que el manual de Gobierno Digital desarrolla el proceso de implementación de la política a través de cuatro grandes momentos:

1. Conocer la política (Evolución, Qué es Gobierno Digital, Propósitos, Elementos, Actores)
2. Planear la política (Cómo planear la política en la Entidad)
3. Ejecutar la política (TIC para el Estado y TIC para la sociedad, Habilitadores Transversales, Apoyo a la Implementación)
4. Medir la política (Seguimiento y evaluación en la entidad, Seguimiento y evaluación MINTIC), los cuales incorporan las acciones que permitirán desarrollar la política en las entidades públicas de nivel nacional y territorial.

En la entidad se evidencia la adopción de la política de seguridad digital en la vigencia 2023 mediante la Resolución N° 036 del 31 de enero de 2023, como se muestra en la siguiente imagen:

TERMINAL METROPOLITANA
de Transporte de Barranquilla S.A.
VOY SEGURO, USO LA TERMINAL

ALCALDÍA DE BARRANQUILLA / Soy BARRANQUILLA

RESOLUCIÓN No 036 DEL 31 DE ENERO DE 2023

POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA DE SEGURIDAD DIGITAL DE LA TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA S.A.

El Gerente de la TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA S.A., en uso de sus facultades Legales, Estatutarias y en especial las conferidas por la Ley 489 de 1998 y demás atribuciones que le confieren los estatutos y las autorizaciones de la Junta Directiva y

CONSIDERANDO

Qué, el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

Que la planificación e implementación del Modelo de Seguridad y Privacidad de la Información MSPI, está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad y conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos,, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Que a través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información y se ha elaborado un conjunto de documentos asociados para estar acorde con las buenas prácticas de seguridad y facilitar su actualización periódicamente teniendo en cuenta los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública.

Que con la expedición del Decreto 1499 de 2017 se estableció un único Sistema de Gestión, Modelo Estándar de Control Interno "MIPG" con la finalidad de mejorar el desempeño y resultado de las Entidades públicas para la satisfacción de las necesidades y goce efectivo de los derechos de los ciudadanos en cumplimiento de la legalidad e integridad.

Que la Terminal Metropolitana de Transportes de Barranquilla S.A. recibe, produce y gestiona diariamente información crucial para el correcto desempeño y cumplimiento de los objetivos institucionales, de ahí que la seguridad y la privacidad de la información revista tal importancia para la alta dirección, para evitar cualquier posibilidad de mal uso o pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios.

Que la Subgerencia de Planeación, Proyectos, Desarrollo y TICs por medio de la Oficina de Sistemas es la responsable de mantener en correcto funcionamiento la plataforma tecnológica de la Terminal metropolitana de Transportes de Barranquilla S.A., así como los sistemas de información de la entidad y de toda la información que formalmente le han sido asignados, para esto ha definido la Política de Seguridad Digital.

de Transporte de Barranquilla S.A.
VOY SEGURO, USO LA TERMINAL

ALCALDÍA DE BARRANQUILLA / Soy BARRANQUILLA

RESOLUCIÓN No 036 DEL 31 DE ENERO DE 2023

POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA DE SEGURIDAD DIGITAL DE LA TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA S.A.

Que, 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.

Que, 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.

Que, para la vigencia, la Terminal Metropolitana de Transportes de Barranquilla S.A., define la Política de Seguridad Digital de la Terminal Metropolitana de Transportes de Barranquilla S.A. la cual es de obligatorio cumplimiento para el personal que hace uso de los servicios digitales.

Que, en mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO. ***ADOPTAR E IMPLEMENTAR*** la Política de Seguridad Digital de la Terminal Metropolitana de Transportes de Barranquilla S.A., de la Terminal Metropolitana de Transportes de Barranquilla S.A., contenida en el presente acto administrativo, y el documento de la política que forma parte integral del presente acto administrativo.

ARTÍCULO SEGUNDO. ***DESIGNAR*** para su verificación de la implementación, seguimiento y control al uso de herramientas informáticas como acciones definidas en el plan de acción a la Oficina de Sistemas.

ARTÍCULO TERCERO. ***PUBLICAR*** en la página web de la Terminal Metropolitana De Transportes De Barranquilla S.A.

ARTÍCULO CUARTO. El presente acto administrativo rige a partir del día de su expedición.

COMUNÍQUESE Y CÚMPLASE

Expedida en el Municipio de Soledad a los treinta y un (31) días del mes de enero de 2023.

RUBEN HERNAN GARCIA ARIZA
Gerente

Proyectó: Claudia Vargas López – jefe Oficina de Sistemas

BARRANQUILLA.GOV.CO

Carrera 14 # 54-186 Módulo D 1er piso - Tel 57 (5) 393 00 43
www.ttbaq.com.co - contacto@ttbaq.com.co
NIT 890.106.084-4 - Soledad - Atlántico

Esto en cumplimiento a la implementación de una de las políticas de gestión y desempeño de MIPG (Modelo Integrado de planeación y gestión)-

Así mismo, se han realizado socializaciones y difusiones de la política de seguridad digital por parte de la oficina de sistemas, a través de correo electrónico, WhatsApp institucional y página web al interior de la entidad, como lo evidenciamos en las siguientes imágenes:

POR CORREO ELECTRONICO

De: Claudia Elizabeth Vargas Lopez <jefesistemas@ttbaq.com.co>
Enviado: viernes, 1 de diciembre de 2023 10:35
Para: ventanilla unica <ventanillaunicaderadicacion@ttbaq.com.co>
Asunto: POLÍTICA DE SEGURIDAD DIGITAL

Buenos días,
Se solicita el envío del adjunto mediante el correo electrónico.

PARA:
FUNCIONARIOS Y CONTRATISTAS
TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA S.A.

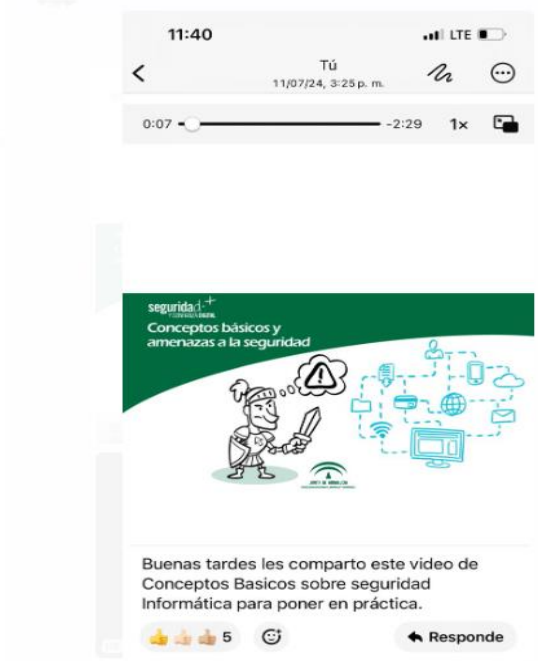
Cordial Saludo,

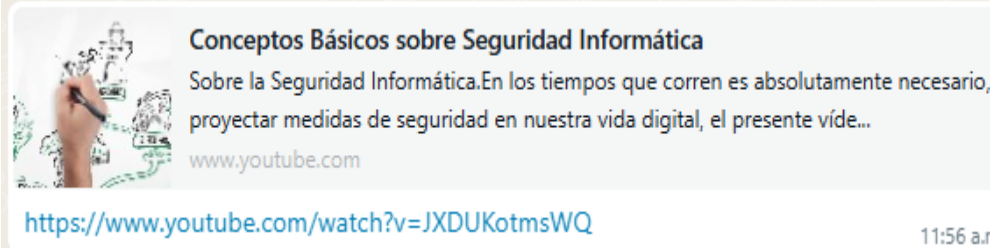
La Oficina de Sistemas se permite dar a conocer su Política de Seguridad Digital para lo cual comparte los siguientes ítems para tener en cuenta:

Cordialmente,

TERMINAL METROPOLITANA
de Transportes de Barranquilla S.A.
CLAUDIA VARGAS LÓPEZ
Cra 14 # 54 - 186 Módulo C - Piso 2
Claudia.vargas@ttbaq.com.co
www.ttbaq.com.co
Cuidemos el medio ambiente, por favor no imprima este correo electrónico si no es necesario

POR WHATSAPP INSTITUCIONAL





De Igual forma, para informar a la comunidad y ciudadanía y con el fin de cumplir con la ley de corrupción Ley 1474 de 2011 y la ley de transparencia 2195 de 2022, esta política de seguridad digital fue publicada en la página web de la entidad de conformidad con el siguiente enlace e imagen:

https://www.ttbaq.com.co/imagesupload/varias2023/POLITICA-DE-SEGURIDAD-DIGITAL.pdf

EJECUCIÓN DE LA POLITICA

Con referencia a la ejecución de la política de seguridad digital encontramos lo siguiente:

La política de Seguridad digital en la entidad consiste en:

"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."

Para dar cumplimiento a lo anterior, se estableció el siguiente alcance. Se muestra el avance de las actividades:

ACTIVIDAD-ALCANCE	RESPONSABLE	ESTADO / AVANCE
Revisar y actualizar los activos de información.	Oficina de Sistemas, la Secretaría General por medio de la Oficina de Atención al Ciudadano y Gestión Documental	Se evidencia la actualización de la matriz de inventario de activos de información de las siguientes oficinas: atención al ciudadano y gestión documental, sistemas, control interno, talento humano y planeación en el siguiente enlace en la pagina web de la entidad. https://www.ttbaq.com.co/Datos%20abiertos/ Se recomienda que la subgerencia operativa, subgerencia financiera, oficina de servicios logísticos y administrativos y secretaria general oficinas elaboren su matriz de inventario de activos de información en cumplimiento de la normatividad legal vigente.
Levantamiento de la infraestructura tecnológica crítica de la entidad	Oficina de sistemas	Se evidencia el catálogo de elementos de infraestructura de tecnología de información, el cual debe ser actualizado a la fecha.

Actualizar los riesgos de seguridad digital siguiendo la metodología dispuesta por el DAFP y Ministerio Tics	Oficina de sistemas	Se evidencia un plan de mejoramiento suscrito con la oficina de control Interno en el cual se establece dentro de las actividades la adopción e implementación del Plan de tratamiento de riesgos y de seguridad de la información, el cual debe ser aprobado por el comité institucional de gestión y desempeño de la entidad
Implementar 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.	Todas las dependencias con el apoyo de la Subgerencia de Planeación, Proyectos, Desarrollo y Tics	Se evidencia un plan de mejoramiento suscrito con la oficina de control Interno en el cual se establece dentro de las actividades la elaboración del Modelo de seguridad y privacidad de la información (MSPI), el cual debe ser aprobado por el comité institucional de gestión y desempeño de la entidad.
Evaluar 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.	La Subgerencia de Planeación, Proyectos, Desarrollo y TICs,	Esta actividad se encuentra en ejecución. A la fecha se evidencia la adopción de la política de seguridad digital en la entidad. Se han realizado socializaciones en la vigencia 2023 y 2024. Se evidencia un plan de mejoramiento suscrito con la oficina de control Interno en el cual se establece dentro de las actividades la adopción e implementación del Modelo de seguridad y privacidad de la información (MSPI) y del Plan de tratamiento de riesgos y de seguridad de la información.
Sensibilizar a usuarios internos en el uso de medios digitales y en buenas	La Subgerencia de Planeación, Proyectos, Desarrollo y TICs	A la fecha se ha realizado por parte de la oficina de sistemas la socialización de la política de seguridad digital (Resolución 036 de 2023), por correo electrónico y el WhatsApp institucional el día 1 de diciembre de 2023.

prácticas para mitigar los riesgos de seguridad digital que puedan afectar a la entidad.		Así mismo para informar a la comunidad y ciudadanía y con el fin de cumplir con la ley de corrupción Ley 1474 de 2011 y la ley de transparencia 2195 de 2022, esta política de seguridad digital fue publicada en la página web de la entidad de conformidad con el siguiente enlace e imagen: https://www.ttbaq.com.co/politicas-lineamientos-y-manuales/

POLITICAS PARTICULARES DE SEGURIDAD DIGITAL

POLITICA	PARÁMETROS	OBSERVACIONES
CORREO CORPORATIVO	• 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 contraseña asignados, de igual manera dicha información debe entregarse cuando exista un proceso de empalme.	Se evidencia el cumplimiento de los parámetros establecidos en la política adicional de correo corporativo. Es importante recordar que cuando un servidor público tiene asignada una cuenta de correo de la entidad, y se desvincula, este debe entregar a la Oficina de Sistemas los usuarios y contraseña asignados, a través de la oficina de talento humano mediante el acta de entrega y/o empalme.
SEGURIDAD PARA EQUIPOS INSTITUCIONALES	• 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	Se evidencia el cumplimiento de los parámetros establecidos en la política adicional sobre la seguridad para equipos institucionales. Se evidencia el formato TIC-F.004 Asignación de equipos de

	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.	computo en donde se asigna a cada funcionario de la entidad el equipo institucional. Así mismo, se evidencian el acta de entrega de el equipo a cada servidor. Cuando es detectada alguna falla o un equipo necesite de reparación, la oficina de sistema realiza copia de seguridad de la información en un disco duro extraíble para evitar la perdida de datos e información. El software (Sistema de información)utilizado en la entidad para recaudo está protegido por derechos de autor y licencia de uso de Consultores tecnológicos Actualmente, los equipos no tienen instalado programa de antivirus, sin embargo, si posee un firewall de correo e internet seguro que detecta la presencia de virus u otro agente potencialmente peligroso. Existe un usuario administrador (Oficina de sistemas) que solo es quién se encarga de la descarga de softwares u otros aplicativos que sean requeridos, para la realización de actividades institucionales

CONTROL DE ACCESO	Tener en cuenta la Política de Control de Acceso definida.	Se evidencia Política Institucional de control de acceso adoptada en mediante Resolución 333 de diciembre de 2022. Se debe realizar la revisión para realizar ajustes en el caso que se requiera. Esta política se encuentra publicada en la página web de la entidad en el siguiente enlace: https://www.ttbaq.com.co/politicas-lineamientos-y-manuales/ Así mismo, debe ser socializada con los usuarios internos de la entidad.
ADMINISTRACION 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.	Cada usuario de la entidad maneja su usuario y contraseña para ingresar al equipo asignado. El usuario administrador (Oficina de sistemas), es el único responsable y encargado de habilitar o deshabilitar contraseñas y permisos o privilegios de acceso para usuarios internos a los sistemas de información utilizados en la entidad. Se requiere seguir revisando periódicamente por parte de la oficina de sistemas los permisos o privilegios de acceso a los diferentes sistemas de información de los servidores públicos y/o contratistas.

ACCESO A INTERNET	• 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.	Se requiere por parte de sistemas el monitoreo permanente en cuanto al acceso de internet por parte de los usuarios internos.

POLITICA DE CONTROL DE ACCESO EQUIPOS

Se evidencia la adopción de la política de control de acceso a equipos, mediante la Resolución N° 333 de diciembre 30 de 2023. Se evidencia socialización de esta política el día 12 de diciembre de 2023 a través de correo electrónico institucional a los funcionarios de la entidad. Como se muestra en la siguiente imagen:

Esta política se encuentra publicada en la página web de la entidad, a través del siguiente enlace: https://www.ttbaq.com.co/imagesupload/varias2023/POL%C3%8DTICA%20DE%20CONTROL%20DE%20ACCESO%20A%20EQUIPOS.pdf

Esta política contiene el, objetivo, alcance, definiciones, directrices de seguridad para el personal, normas de seguridad para el control de acceso lógico y acceso físico, y responsabilidades.

Directrices de seguridad para todo el personal		
Directriz	**Responsable**	**Observaciones**
Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información	Oficina de sistemas	Esta política se cumple ya que la oficina de sistemas asigna el nombre de usuario a cada funcionario para pode r acceder a los sistemas de información utilizados en la entidad
Se deberá deshabilitar los usuarios correspondientes al personal que ya no tenga relación con la entidad.	Oficina de sistemas	La oficina de sistemas como administrador de usuarios, es únicamente el encargado de deshabilitar los usuarios correspondientes al personal que no tiene relación con la entidad

Para generar acceso físico y/o lógico a funcionarios, la Oficina de Talento Humano debe realizar la solicitud al área respectiva.	Oficina de Talento Humano	Aunque esta actividad se realiza por parte de la oficina de sistemas y oficina de servicios administrativos y logísticos. Se requiere que la oficina de talento humano realice formalmente la solicitud al área respectiva.
Para generar acceso físico y/o lógico a contratistas, el supervisor del contrato debe realizar la solicitud al área respectiva.	Supervisor del Contrato	Aunque esta actividad se realiza por parte de la oficina de sistemas y oficina de servicios administrativos y logísticos. Se requiere el supervisor del contrato realice formalmente la solicitud al área respectiva.
Cuando se presente desvinculación de un funcionario, la Oficina de Talento Humano debe informar a la Oficina de Sistemas con el fin de que se proceda con la deshabilitación de los usuarios y a la Oficina de Servicios Administrativos y Logísticos para la restricción de acceso físico.	Oficina de talento humano/ oficina de sistemas	Aunque esta actividad se realiza por parte de la oficina de sistemas y oficina de servicios administrativos y logísticos. Se requiere solicitarse de manera formal por el área de talento humano a la oficina de sistemas y/o servicios logísticos.
Es responsabilidad del supervisor, solicitar la cancelación de los derechos de acceso físico y/o lógico cuando el contratista haya finalizado la ejecución de los servicios contratados.	Supervisor del contrato	Se requiere el supervisor del contrato realice formalmente la solicitud al área respectiva.
Se deberán realizar revisiones periódicas en los diferentes sistemas de información para garantizar que se remuevan los usuarios deshabilitados o redundantes.	Oficina de sistemas	Esta actividad se realiza de manera periódica por la oficina de sistemas
Cada funcionario y/o contratista de la entidad es responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información, así como de las acciones realizadas con los mismos.	Funcionario/ contratista	Se evidencia cumplimiento
El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.	Funcionario	Se evidencia cumplimiento

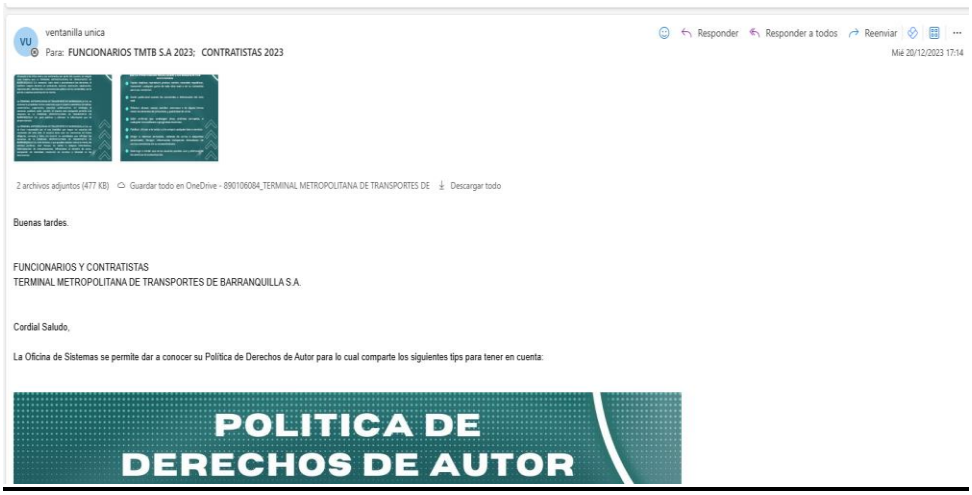
Directrices de seguridad para el control de acceso lógico		
Directriz	**Responsable**	**Observaciones**
Los líderes de procesos deberán ser los únicos autorizados para solicitar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario.	Lideres de procesos	Se requiere que el líder del proceso respectivo realice la solicitud al área de sistemas de manera formal.
La administración de los perfiles de usuario es responsabilidad de la oficina de sistemas y del jefe de área o supervisor que realice la solicitud de asignación de usuarios. La Oficina de Sistemas es la encargada de crear, modificar, bloquear o eliminar cuentas de usuarios de red, sistemas de información y demás recursos tecnológicos según lo requerido por los jefes de las demás dependencias.	Oficina de sistemas	Esta actividad se realiza por la oficina de sistemas quien es el usuario administrador, quien se encarga de crear, modificar, bloquear o eliminar cuentas de usuarios de red, sistemas de información y demás recursos tecnológicos según lo requerido
Se deberá establecer un procedimiento de entrega de usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red de la Terminal Metropolitana de Transportes de Barranquilla, a los recursos tecnológicos o a los sistemas de información.	Oficina de sistemas	Se evidencia el Procedimiento TIC-P-003 Administración de usuarios, de la oficina de sistemas, aprobado por la oficina de planeación
Se deberá verificar periódicamente las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso a los recursos tecnológicos y sistemas de información de la SSF.	Oficina de sistemas	Se recomienda a la oficina de sistemas realizar la verificación y validación periódica de las novedades del personal relacionadas con la eliminación reasignación o bloqueo de cuentas de acceso a los recursos y sistemas de información.

Directrices de seguridad para el control de acceso físico		
Directriz	**Responsable**	**Observaciones**
Se deberá identificar al personal que requiere acceso a las oficinas administrativas, autorizar su ingreso y conceder los privilegios necesarios para el acceso físico.	Oficina de servicios administrativos y logísticos	Se cumple con la directriz
Se deberá contar con mecanismos de control de acceso para las áreas seguras (el datacenter); para controlar el acceso al este.	Oficina de servicios administrativos y logísticos / oficina de sistemas	Se cumple con la directriz
Las puertas de acceso al datacenter, centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.	Oficina de servicios administrativos y logísticos / oficina de sistemas	Se cumple con la directriz
Se deberá aprobar de manera previa las solicitudes de acceso de terceros al datacenter, además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.	Oficina de servicios administrativos y logísticos / oficina de sistemas	Se cumple con la directriz
Se deberá monitorear los ingresos al centro de cómputo permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.	Oficina de servicios administrativos y logísticos / oficina de sistemas	Se cumple con la directriz
Se deberá bloquear de manera inmediata los privilegios de acceso físico a las oficinas administrativas de la Terminal Metropolitana de Transportes de Barranquilla tan pronto el personal termine su vinculación.	Oficina de servicios administrativos y logísticos / oficina de sistemas	Se cumple con la directriz

Se hace necesario que esta política sea revisada y ajustada si se requiere y nuevamente socializada, por parte de la oficina de sistemas.

POLITICA DE DERECHOS DE AUTOR

Se evidencia la adopción de la política de derechos de autor mediante la Resolución N° 218 de agosto 02 de 2023. Se evidencia socialización de esta política el día 20 de diciembre de 2023 a través de correo electrónico institucional a los funcionarios de la entidad. Como se muestra en la siguiente imagen:



Esta política se encuentra publicada en la página web de la entidad, a través del siguiente enlace: https://www.ttbaq.com.co/imagesupload/varias2023/POLITICA-DE-DERECHOS-DE-AUTOR.pdf

Esta política contiene el alcance y límites de uso, los derechos de la entidad, la responsabilidad de los usuarios, así mismo, se especifica sobre el medio, a través del cual debe ser enviada cualquier notificación de reclamo o violación de los derechos de propiedad bajo la ley colombiana

Se hace necesario que esta política sea socializada nuevamente en la vigencia 2024, por parte de la oficina de sistemas.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCION DE DATOS

Se evidencia una política de seguridad de la información y protección de datos de la vigencia 2016, la cual se encuentra publicada en la página web de la entidad según el siguiente enlace:

https://www.ttbaq.com.co/imagesupload/varias/Pol_tica_de_seguridad_y_protecci_n_de_datos_person.pdf

Esta política debe ser revisada y actualizada conforme al plan de mejoramiento suscrito por la oficina de sistemas en la vigencia 2024 con la oficina de control interno, en el cual como actividad se establece la elaboración y aprobación del Plan de Tratamiento de riesgos de seguridad y privacidad de la información y el plan de seguridad y privacidad de la información en cumplimiento de la normatividad vigente.

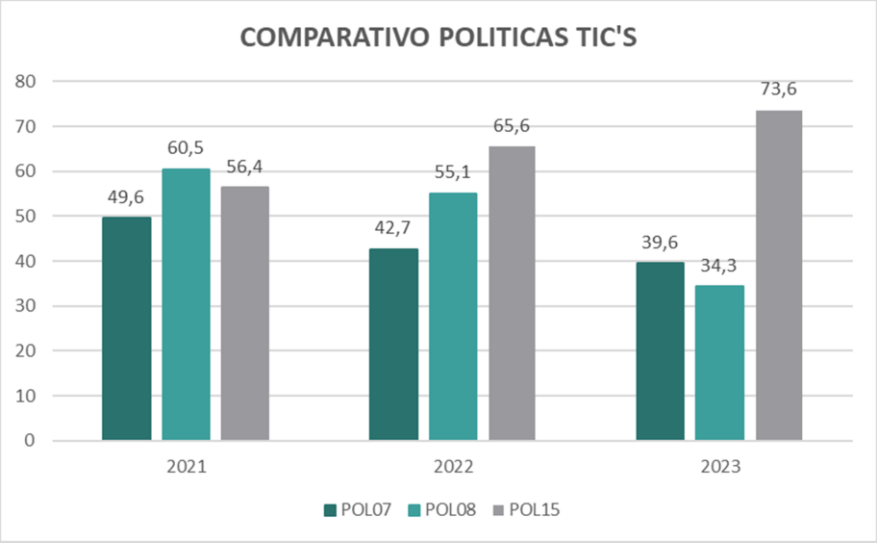
MEDICIÓN DE LOS RESULTADOS DEL FURAG

Estas políticas deben ser evaluadas a través del aplicativo de la función pública FURAG (Formulario Único de Reportes de Avance de la Gestión). Según el reporte del FURAG, sobre el Índice de Desempeño Institucional vigencia 2023, suministrado por la oficina de planeación encontramos los siguientes resultados:

RESULTADOS POR DIMENSIONES Y POLÍTICAS DE GESTIÓN Y DESEMPEÑO

D1: TALENTO HUMANO	-	54,5	65,1	80
POL01: Gestion Talento Humano	41,09	47,5	83,9	**90,4**
POL02: Integridad	62,4	62,4	55,9	**73,2**
D2: DIRECCIONAMIENTO ESTRATEGICO Y PLANEACION	-	60	71	82
POL03: Planeacion institucional	62,2	60	67,4	**82,3**
D3: GESTION DE RESULTADOS	-	56	44,1	49
POL05: Compras y contratación publica	N/A	N/A	80,6	N/A
POL06: Fortalecimiento organizacional y simplificación de procesos	45,1	49,7	82,3	**85,9**
D4: EVALUACION DE RESULTADOS	-	56	51,9	51,2
POL07: Gobierno Digital	44,1	49,6	42,7	39,6
POL08: Seguridad Digital	64,1	60,5	55,1	34,3
POL11: Servicio al ciudadano	50,2	53	37,6	**52,3**
POL12: Racionalización de tramites	50	51,7	19,1	18,2
POL13: Participacion ciudadana	55,8	56,3	41,8	**50,2**
POL14: Seguimiento y evaluacion del desempeño institucional	66,9	47,8	51,9	**52,1**

PROCESO FORTALECIMIENTO DE LAS TICS (COMPARATIVO DE LAS VIGENCIAS)



PO7 GOBIERNO DIGITAL - P08 SEGURIDAD DIGITAL

De conformidad con los gráficos anteriores, observamos que la política de gobierno y seguridad digitales obtuvieron un porcentaje de avance de 39.6% y 34.3%de respectivamente. Así mismo, se evidencia una disminución en el cumplimiento de las políticas en la vigencia 2023 con respecto a las anteriores vigencias (2022 y 2021), esto debido al establecimiento de las nuevas directrices y lineamientos del gobierno nacional y del Ministerio de las Tecnologías de la información y comunicaciones en la vigencia 2022 y 2023, referentes a gobierno digital, seguridad de la información y ciberseguridad, ya que a la fecha no se han ejecutado en su totalidad.

De igual forma, se evidencia plan de mejoramiento suscrito a la oficina de Control interno, referente a las recomendaciones dadas por la Función Pública en los resultados del Índice de Desempeño Institucional del aplicativo FURAG. Como se muestra en la siguiente imagen:

	FORMULACION Y SEGUIMIENTO PLAN DE MEJORAMIENTO PROCESOS
Nombre de la Entidad:	Terminal Metropolitana de Transporte de Barranquilla S.A.
Representante Legal:	Liliana Rosales Dominguez
Auditoria Nº:	Resultados FURAG 2023
Jefe y/o Lider del proceso	Eimy Barrios Garcia
Periodo Fiscal que cubre:	2023
Fecha de Suscripción:	25/09/2024
Fecha de Evaluación del plan:	31/12/2024

DESCRIPCION DEL HALLAZGO(No mas de 50 palabras)	CAUSA DEL HALLAZGO	ACCION DE MEJORAMIENTO	RESPONSABLE	META	UNIDAD DE MEDIDA DE LA META	FECHA INICIACION DE METAS	FECHA TERMINACION DE METAS
Falta implementación de actividades y requisitos de la Política de Gobierno digital por parte del responsable de la Política	Por desconocimiento de las actividades propias de la política	Capacitar al personal de la entidad (Contratistas y servidores) en las actividades propias de la Política de Gobierno Digital	Jefe de Oficina de Sistemas	1 procedimiento realizado y aprobado	Procedimiento	25/09/2024	30/06/2025
		Actualizar las actividades propias del Plan de seguridad y privacidad de la información	Jefe de Oficina de Sistemas / Oficina de Talento Humano	1 Capacitación realizada	Registro de asistencia a las socializaciones / Registros fotograficos	25/09/2024	30/06/2025
		Actualizar las actividades propias del Plan de seguridad y privacidad de la información	Jefe de Oficina de Sistemas	Plan de seguridad y privacidad de la información	Plan Aprobado, acta de comité	25/09/2024	30/06/2025
		Formulación de matriz de riesgos de seguridad y privacidad de la información para la TMTBAQ	Jefe de Oficina de Sistemas	Matriz de riesgo formulada	Acta de aprobación del comité de gestión y desempeño	25/09/2024	30/06/2025
No implementar el Plan de Recuperación de desastres DRP, exigido por la política de seguridad digital	Por desconocimiento de los requisitos de la política de seguridad digital	Implementación y aprobación del Plan de Recuperación de desastres DRP de la entidad	Jefe de Oficina de Sistemas	Plan de recuperación de desastres aprobado	Acta de aprobación del comité de gestión y desempeño	25/09/2024	30/06/2025

Estas actividades se encuentran en ejecución y el plazo máximo establecido para su implementación es hasta el 30 de junio de 2025, por parte de la oficina de sistemas.

CONCLUSIONES Y RECOMENDACIONES

La oficina de sistemas anualmente debe realizar el autodiagnóstico de la política de Gobierno digital según las directrices de la función publica y con base en el autodiagnóstico establecer el plan de acción de su proceso.

La oficina de sistemas debe realizar seguimiento periódico al Plan estratégico de las Tecnologías de la información (PETI), con el fin de seguir trabajando en la implementación de las actividades establecidas, en cumplimiento de la normatividad vigente (Decreto 612 de 2018). Este plan debe revisarse y actualizarse anualmente (cuando se requiera), para ser aprobado en el Comité Institucional de Gestión y desempeño.

En cumplimiento del alcance de la política de seguridad digital establecida, se requiere lo siguiente:

- La subgerencia operativa, subgerencia financiera, oficina de servicios logísticos y administrativos y secretaria general elaboren la matriz de inventario de activos de información en cumplimiento de la normatividad legal vigente y publicarlo en la pagina web, con el seguimiento y aprobación de secretaria general y la oficina de atención al ciudadano y gestión documental.
- Revisar y actualizar el catálogo de elementos de infraestructura de tecnología de información establecido, con el fin de realizar el levantamiento de la infraestructura tecnológica crítica de la entidad.
- Elaborar el Modelo de seguridad y privacidad de la información (MSPI), el cual debe ser aprobado por el comité institucional de gestión y desempeño de la entidad.
- Sensibilizar periódicamente al usuario interno, sobre el uso de medios digitales y de las buenas prácticas para mitigar los riesgos de seguridad digital que puedan afectar a la entidad.

Las políticas de seguridad digital, derechos de autor y control de acceso a equipos se encuentran adoptadas por los actos administrativos correspondientes, socializadas y publicadas en la página web de la entidad; sin embargo, estas deben ser revisadas por la oficina de sistemas, actualizadas de conformidad con los nuevos lineamientos del gobierno (cuando se requiera).

Es necesario, además, que estas políticas sean socializadas periódicamente con los usuarios internos, como una etapa fundamental para su implementación.

Con referencia a la política de seguridad de la información y protección de datos aprobada en la vigencia 2016, esta política debe ser revisada y actualizada teniendo en cuenta el plan de mejoramiento suscrito por la oficina de sistemas en la vigencia 2024 con la oficina de control interno, en el cual como actividad se establece la elaboración y aprobación del Plan de Tratamiento de riesgos de seguridad y privacidad de la información y el plan de seguridad y privacidad de la información.

Se requiere el cumplimiento de los planes de mejoramiento suscritos con la oficina de Control Interno referentes a la elaboración del Plan de tratamiento de riesgos de seguridad y privacidad de la información, Plan de seguridad y privacidad de la información y de las recomendaciones del FURAG para política de Gobierno y seguridad digital.

EDILSA VEGA PEREZ
Asesor Oficina Control Interno