PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TERMINAL METROPOLITANA DE TRANSPORTE DE BARRANQUILLA S.A.

AÑO 2019

1. PRESENTACIÓN

El presente plan de tratamiento de riesgos de seguridad y privacidad de la información, se elabora con el fin de promover dentro de la TTBQA el compromiso de proteger la información que recibe, gestiona y produce la entidad, logrando que las partes interesadas tengan mayor confianza en la entidad, por el adecuado tratamiento de la información que almacenamos.

La Terminal Metropolitana de Transportes de Barranquilla S.A. recibe, produce y gestiona información 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.

De acuerdo con lo anterior, dentro del marco del Modelo de Seguridad y Privacidad de la Información –MSPI, para la gestión de riesgos de seguridad y privacidad de la información, la Terminal Metropolitana de Transportes de Barranquilla S.A. aplicará su política institucional de administración del riesgo, basada en la “Guía Metodológica para la Administración Riesgos y Diseño de Controles” de la función pública versión 4 (octubre de 2018).

Como corolario de lo anterior, el área de sistemas de la TTBQA coordinará la implementación del mapa de riesgos de seguridad digital y privacidad de la información, y el monitoreo sobre las acciones establecidas para controlar o administrar los riesgos.

La TTBAQ acoge la gestión de riesgos como un proceso sistemático para su identificación, análisis, evaluación, valoración, y tratamiento; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad de la información de los usuarios, funcionarios, proveedores y empresas transportadoras

2. ADMINISTRACIÓN DE RIESGOS SOBRE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Administración de riesgos de seguridad y privacidad de la información es un método sistemático que permite a las organizaciones identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura que almacenan y procesan datos de las operaciones de la entidad y datos personales de los usuarios que con ésta interactúan, permitiéndoles a las entidades minimizar perdidas y maximizar oportunidades.

No hay que olvidar que toda infraestructura tecnológica que almacena datos está expuesta de daños, ataques cibernéticos u obsolescencia que representan un gran riesgo para las organizaciones, aunado a ello, el mal uso que los administradores de los sistemas de información o bases de datos pudieran hacer sobre la información que almacena la entidad.

Para la administración del riesgo de seguridad y privacidad de la información en la Terminal de Transportes se conciben tres elementos a saber: i) la **Divulgación** y apropiación de la política de seguridad y protección de datos personales de la Terminal Metropolitana de Transportes de Barranquilla S.A., ii) el **Código de Integridad** del servicio público adoptado por la TTBAQ y iii) la **Política institucional de administración de riesgos** 2018 de la TTBAQ.

3. RESPONSABLE DE LA ADMINISTRACIÓN DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El área de sistemas será el responsable de la administración de los riesgos de seguridad y privacidad de la información, a partir del diligenciamiento de la herramienta “mapa de riesgos integrados”, su monitoreo y seguimiento. De conformidad con la política institucional de administración del riesgo, cuando éstos se encuentren en **zona alta y extrema** deberán integral el mapa de riesgos institucional y será objeto de seguimiento por parte del Comité Institucional de Control Interno.

4. PRINCIPIOS DE LA PROTECCIÓN DE LA INFORMACIÓN

- **Confidencialidad:** únicamente las personas autorizadas tienen acceso a la información sensible o privada.
- **Integridad:** la información y los métodos de procesamiento de esta información son exactos y completos, y no se han manipulado sin autorización.
- **Disponibilidad:** los usuarios que están autorizados pueden acceder a la información cuando lo necesiten.
- **Autenticidad:** sólo los usuarios autenticados pueden gestionar la información según los perfiles o permisos creados.
- **Identidad:** hay garantía de la autoría de una determinada acción y está asociada a quien ha producido esta acción.

5. AMENAZAS EN LA SEGURIDAD DE LA INFORMACIÓN

Las amenazas pueden afectar diferentes aspectos de la seguridad de los activos de información, por tanto uno de nuestros objetivos es el análisis de qué amenazas pueden afectar los activos de la Terminal Metropolitana de Transportes de Barranquilla S.A. A continuación se exponen algunas amenazas potenciales que hemos identificadas por tipo:

Según la operación de los equipos

- Daño en los equipos y servidores por falta de mantenimiento
- Alteración o eliminación de base de datos de los procesos

Según el hardware

- Alteración, suplantación, eliminación o Divulgación Datos Servidor correo
- Pérdida o robo Dispositivos móviles

- Daño o alteración Equipos de Escritorio
- Daño, alteración o fuga de información Equipos Portátiles
- Daño o alteración Impresoras
- Daño, alteración o fuga de información Servidor Aplicaciones
- Daño, alteración o fuga de información Servidor backup
- Daño, alteración o fuga de información Servidor Bases de datos
- Daño, alteración o fuga de información Servidor de correo Malware, troyano, gusanos, descargas o visitas a través de Unidades extraíbles

Según el software

- Daño en aplicación o sistemas operativos
- Daño o alteración aplicaciones ofimática
- Alteración, eliminación o divulgación base de datos de contraseñas
- Alteración, suplantación o eliminación correo electrónico
- Alteración, eliminación o divulgación datos backup
- Alteración, eliminación o divulgación programas de administración (contabilidad, tesorería, presupuesto, oficina de conduce, manejo de personal, etc.)
- Daño o alteración programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)
- Alteración, eliminación o divulgación programas de producción de datos
- Alteración, eliminación o divulgación programas manejo documental
- Daño o alteración servidor antivirus
- Daño, alteración o fuga de información

Según la Red

- Daño o alteración Equipos de la red cableada (router, switch, etc.)
- Daño o alteración Equipos de la red inalámbrica (router, punto de acceso, etc.) Malware, troyano, gusanos, descargas o visitas a través de Navegación en Internet inclusiones a PBX (Sistema de telefonía convencional)
- Daño o alteración Servidor Firewall

6. RIESGOS SEGURIDAD DE LA INFORMACIÓN

Algunos riesgos identificados en el proceso de seguridad de información son los siguientes:

- Daños en los equipos por situaciones adversas
- Daños en red y equipos causados por cortos circuitos
- Susceptibilidad del hardware a las variaciones de voltaje
- Copia no controlada del hardware
- Ausencia de “terminación de sesión” cuando se abandona el puesto de trabajo.
- Disposición o reutilización de los medios de almacenamiento sin borrado adecuado en el software
- Asignación errada de los derechos de acceso al software
- Configuración incorrecta de parámetros en el software
- Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario del software
- Ausencia de copias de respaldo del software
- Arquitectura insegura de la red
- Uso incorrecto de software y hardware
- Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
- Ubicación en área susceptible de lluvia
- Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
- Ausencia de auditorías de sistemas
- Ausencia de políticas sobre el uso de correo electrónico
- Ausencia de control de los activos que se encuentran fuera de las instalaciones
- Carencia de protocolo de manejo interno de la información magnética.
- Red de cableado obsoleta y falta de mantenimiento.
- Adquisición de tecnologías que no aportan valor a la organización
- No contar con presupuesto suficiente para la ejecución de proyectos encaminados a la parte tecnológica

7. DIAGNÓSTICO DE CONDICIONES DE SEGURIDAD

Además de la gestión de los riesgos de seguridad de la información se deberá desarrollar un diagnóstico sobre la situación de seguridad de los equipos, sistemas de información y bases de datos teniendo en cuenta entre otros, los siguientes aspectos.

- Control de acceso y restricciones en los equipos y bases de datos.
- Eficiencia de los planes de mantenimiento preventivos.
- Elaboración de copias de seguridad.
- Gestión de Incidentes de Seguridad de la Información.
- Mecanismos de protección de malware, spyware, gusanos, troyanos, rootkits, etc.
- Competencias adecuadas de los servidores que administran los equipos, sistemas de información y bases de datos.
- Adecuada operación de los equipos servidores.

8. PLAN DE ACCIÓN DE SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN.

El resultado del diagnóstico de las condiciones de seguridad y de la administración del riesgo conlleva a un "**Plan de acción – cronograma"** que establezca las actividades a desarrollar para atender las debilidades extractadas de los diagnósticos, atender las oportunidades, optimizar las fortalezas y controlar los riesgos.

Para el diagnóstico de condiciones de seguridad y formulación del plan de acción se deberán observar los lineamientos del procedimiento de diagnóstico y plan de acción de seguridad de la información y el formato de plan de acción correspondiente.

Adicionalmente, el Plan de acción de seguridad y protección de la información deberá integrarse al plan de acción del proceso.

9. MONITOREO, EVALUACIÓN Y SEGUIMIENTO.

El monitoreo del plan de acción de seguridad y protección de la información estará a cargo del área de sistemas, y el control, a cargo de la Oficina de Control Interno, de conformidad con las líneas de auditoría que esta desarrolle y de acuerdo con su Plan de Auditorías.