Resolución Número 429
(Julio 17 de 2020)

"Por la cual se adopta el documento P-DT-018 Procedimiento para gestionar las vulnerabilidades tecnológicas"

EL JEFE DE LA OFICINA ASESORA DE PLANEACIÓN DE LA EMPRESA DE TRANSPORTE DEL TERCER MILENIO "TRANSMILENIO S.A.",
En uso de sus facultades conferidas mediante la Resolución 342 del 16 de junio de 2020, y

CONSIDERANDO:

Que de conformidad con lo señalado en el artículo segundo del Acuerdo 4 de 1999, corresponde a TRANSMILENIO S.A., la gestión, organización y planeación del servicio de transporte público masivo urbano de pasajeros en el Distrito Capital y su área de influencia, bajo la modalidad de transporte terrestre automotor.

Que cumpliendo con lo ordenado en el parágrafo único del artículo 1º de la Ley 87 de 1993, se adoptó el Manual de Procedimientos de TRANSMILENIO S.A.

Que, siendo TRANSMILENIO S.A., el ente gestor del Sistema Integrado de Transporte Público, considera necesario actualizar los Manuales de Procedimientos de las diferentes dependencias de la Entidad, con el objeto de ajustarlos a los nuevos parámetros documentales, necesidades y desarrollo del Sistema.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°: Adoptar el siguiente documento con el nombre, código y versión que se registran a continuación:

CÓDIGO	VERSIÓN	NOMBRE
P-DT-018	0	Procedimiento para gestionar las vulnerabilidades tecnológicas

ARTÍCULO 2°: La presente Resolución rige a partir de su publicación en la Gaceta Distrital.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., a los diecisiete (17) días del mes de julio de dos mil veinte (2020).

SOFÍA ZARAMA VALENZUELA
Jefe de Oficina Asesora de Planeación

TABLA DE CONTENIDO

1. OBJETIVO 2

2. ALCANCE 2

3. RESPONSABLES 2

4. DOCUMENTOS DE REFERENCIA 2

5. DEFINICIONES 4

6. CONDICIONES GENERALES 5

6.1 Clasificación de las vulnerabilidades 6

7. DESCRIPCIÓN DEL PROCEDIMIENTO 6

8. TABLA DE FORMATOS 9

1. OBJETIVO

Definir los pasos que se deben seguir para detectar, analizar, priorizar y corregir las vulnerabilidades presentes en los componentes tecnológicos que soportan los procesos del negocio de TRANSMILENIO S.A. lo anterior, con el fin de reducir los riesgos a los que está expuesta la información y así mismo cumplir con los requerimientos regulatorios que aplican a la entidad.

2. ALCANCE

El procedimiento inicia con la identificación de activos de tecnología y finaliza con el seguimiento a la remediación de las vulnerabilidades. Así mismo, el documento cubre todos los componentes de la infraestructura tecnológica de TRANSMILENIO S.A.

Debe ser aplicado por todos los funcionarios y contratistas que realicen la administración y gestión de los activos tecnológicos de la entidad.

3. RESPONSABLES

El Profesional Especializado Grado 06 de Seguridad de la Información de la Dirección de TIC es responsable por la elaboración, mantenimiento e implementación de este documento, el Director de Tecnologías de la Información y Comunicaciones será responsable por su cumplimiento.

Se deberá realizar la revisión y/o actualización de este documento cuando los responsables de su aplicación y cumplimiento lo estimen pertinente.

4. DOCUMENTOS DE REFERENCIA

- **Constitución Política de Colombia de 1991**

Artículo 2.	Fines Esenciales del Estado.
Artículo 6.	Responsabilidad de los servidores públicos.
Artículo 15.	Derecho a la Intimidad. Hábeas Data.
Artículo 20.	Derecho a la Información.
Artículo 74.	Libre Acceso a Documentos Públicos.
Artículo 122.	Desempeño de Funciones Públicas.
Artículo 123.	Desempeño de funciones de los Servidores Públicos.
Artículo 209.	Fines de la Función Administrativa.
Artículo 269.	Métodos y Procedimientos de Control Interno.
Artículo 284.	Acceso a Información Reservada.

- **Ley 1273 de 2009.** Por medio del 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, el cual establece en su “Capítulo I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” así:
  - ✓ Artículo 269A
  - ✓ Artículo 269B.
  - ✓ Artículo 269C
  - ✓ Artículo 269D
  - ✓ Artículo 269E
  - ✓ Artículo 269F
  - ✓ Artículo 269G
- **Ley 23 de 1982:** Sobre Derechos de Autor.
- **Ley 527 de 1999.** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 603 del 2000.** Por la cual se modifica el artículo 47 de la Ley 222 de 1995 emitida por el Congreso de la República de Colombia, acerca del cumplimiento de las Normas de Propiedad Intelectual
- **Ley 1520 de 2012.** Por medio de la cual se implementan compromisos adquiridos por virtud del "Acuerdo de Promoción Comercial", suscrito entre la República de Colombia y los Estados Unidos de América y su "Protocolo Modificatorio, en el Marco de la Política de Comercio Exterior e Integración Económica"
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contendida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan 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 acerca de la protección de los derechos de los usuarios.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales, habeas data.
- **Decreto 1360 de 1989.** Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.

- **Decreto 460 de 1995.** Por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal

- **Decreto 162 de 1995.** Por el cual se reglamenta en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos

- **BS ISO/IEC 27001:2013** Norma técnica que describe los requerimientos del Sistema de Seguridad de la Información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado por la ISO International Organization for Standardization y por la IEC International Electrotechnical Commission.

- **BS ISO/IEC 27002:2013** Documento que recopila el código de práctica y los controles para la gestión de la seguridad de la información (Information technology - Security techniques - Code of practice for information security management) aprobado y publicado por la ISO International Organization for Standardization y por la IEC International Electrotechnical Commission.

- **NTC ISO 9001:2015** Norma técnica que determina los requisitos para un Sistema de Gestión de la Calidad (SGC), que pueden utilizarse para su aplicación interna por las organizaciones, sin importar si el producto o servicio lo brinda una organización pública o empresa privada, cualquiera que sea su tamaño, para su certificación o con fines contractuales.

5. DEFINICIONES

Las definiciones mencionadas a continuación son tomadas de la norma ISO27000:2018 y adaptadas para el contexto en el cual TRANSMILENIO S.A. pretende interpretar el presente procedimiento.

Activo: componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa. La entidad asigna un valor a cada activo que representa el nivel de importancia que tiene el activo en el proceso del negocio.

Amenaza: un agente representa una amenaza para un sistema cuando dicho sistema tiene una vulnerabilidad que un atacante puede explotar para obtener un beneficio.

Confidencialidad: garantía de que únicamente accederán a la información los elementos autorizados para ello, y que dichos elementos no van a convertir esa información en disponible para otras entidades.

Disponibilidad: garantía de que la información y los activos relacionados deben estar accesibles a elementos autorizados en tiempo, modo y lugar adecuado.

Integridad: garantía de que la información únicamente puede ser modificada por elementos autorizados asegurando métodos de proceso exactos y completos.

Riesgo: probable ocurrencia de que un atacante explote un fallo de seguridad en un activo determinado, en base a las amenazas existentes y al impacto potencial que representaría para el negocio de la compañía.

Sistema de información: cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales, así como el software, firmware o hardware que forme parte del sistema.

Software: programa de computador.

Solución de errores conocidos: serie de pasos previamente establecidos que permiten resolver un problema en un equipo tecnológico o un Software.

Vulnerabilidad: debilidad o defecto en las Tecnologías de Información que hace que la seguridad (en términos de Confidencialidad, Integridad y Disponibilidad) de un activo sea susceptible de ser comprometida.

Vulnerabilidades Potenciales: vulnerabilidades potenciales incluyen todas las vulnerabilidades que no podemos confirmar existir. La única manera de verificar la existencia de estas vulnerabilidades sería llevar a cabo una exploración intrusiva en su red, lo que podría resultar en una denegación de servicio. Esto está totalmente en contra de nuestra política.

Administradores de los componentes tecnológicos: Administran, configuran y son responsables de las plataformas tecnológicas como servidores, sistemas operativos o sistemas de información.

6. CONDICIONES GENERALES

Las actividades del presente documento tienen como objetivo reducir los riesgos asociados a las vulnerabilidades detectadas en los activos tecnológicos de la entidad, siendo estos quienes soportan los servicios prestados por TRANSMILENIO S.A.

Los servicios de pruebas de vulnerabilidad dentro de TRANSMILENIO S.A podrán subcontratarse o ejecutarse por personal interno siempre que se siga el presente procedimiento.

Algunas de las siguientes metodologías podrán ser utilizadas para la ejecución de las pruebas de vulnerabilidad dependiendo de lo definido dentro del plan de pruebas.

- OSSTMM
- ISSAF
- CEH
- OWASP

Los informes de resultados de los análisis de vulnerabilidades son clasificados como confidenciales y únicamente podrán entregarse al ente respectivo que lo solicite previa autorización del Director de TIC.

Por el desarrollo, ejecución y monitoreo del procedimiento serán responsables los profesionales encargados de la Seguridad de la información de la Dirección de TIC.

6.1 Clasificación de las vulnerabilidades

Las vulnerabilidades se clasifican de acuerdo con los siguientes niveles.

- **Extremo:** La explotación de una vulnerabilidad con nivel Extremo podría proporcionar acceso a datos y sistemas no autorizados, a un nivel de administración.

  El riesgo contempla la exposición de información sensible, tal como identificadores de usuario (nombres), contraseñas, información propietaria, secretos, números de tarjetas de crédito, información de clientes, de colaboradores u otra información sensible de la organización. Así mismo, podría llegar a generar Denegación de Servicio que impacte de manera importante la continuidad de las operaciones.

- **Alto:** La explotación de una vulnerabilidad con nivel Alto podría proporcionar acceso a datos y sistemas no autorizados, en la mayoría de los casos a un nivel administrativo o usuario avanzado.

- **Medio:** La explotación de vulnerabilidades con nivel Medio podría permitir indirectamente acceso a archivos de configuración, datos, o afectar parcialmente un sistema de información.

- **Bajo:** La explotación de una vulnerabilidad con nivel Bajo podría permitir a un atacante obtener información estadística de un sistema, cuentas de usuarios u otra información que podría ser usada para crear un nuevo vector de ataque.

- **Informativo**: Los intrusos pueden reunir información acerca de puertos abiertos y servicios. En este caso, el atacante puede ser capaz de planear nuevos ataques a la infraestructura tecnológica.

7. DESCRIPCIÓN DEL PROCEDIMIENTO

ETAPA	ACTIVIDAD	RESPONSABLE
10	**Inicio**	
20	**Planificar las pruebas.** En esta etapa se deben determinar todos los requerimientos necesarios para realizar las pruebas, así como definir los equipos objeto de las mismas. Lo anterior, teniendo en cuenta aspectos como:	Profesional Especializado Grado 6 - Seguridad informática y

ETAPA	ACTIVIDAD	RESPONSABLE
	• Ubicaciones desde donde se ejecutarán las pruebas. • Sedes y número de dispositivos por cada sede o tecnologías empleadas. • Tipo de pruebas (Escaneos con usuario/contraseña, pruebas de penetración de caja negra, gris o blanca). • Resultados de las evaluaciones de vulnerabilidades realizadas anteriormente en la entidad. Se dejará como registro de esta actividad un Correo electrónico o acta de reunión	Grupo de seguridad de la información
30	**Validación de infraestructura a evaluar** En esta etapa se debe definir y verificar con los administradores de los componentes tecnológicos de la entidad: • Los equipos que serán evaluados como alcance de las pruebas. • Fechas y horarios para le ejecución de las pruebas. • Criticidad de los equipos. • Ambientes de pruebas que deban evaluarse a cambio de los ambientes de producción. Se dejará como evidencia de esta etapa un Correo electrónico o acta de reunión	Grupo de seguridad de la información
40	**Documentar el plan de pruebas.** Se deben realizar las siguientes actividades: • Documentar el plan de trabajo de la ejecución de las pruebas. • Definir el cronograma para la elaboración de las pruebas de acuerdo con las fechas proporcionadas por los administradores de las plataformas. • Solicitar aprobación del plan de trabajo a los administradores.	Grupo de seguridad de la información
¿15?	**¿Se aprueba el plan de pruebas?** **Si:** aprobar el Plan de pruebas de vulnerabilidad e ir a etapa 60 **No:** ir a etapa 50	Profesional Especializado Grado 6 - Seguridad informática
50	**Ajustes Plan de pruebas** Diligenciar y solicitar los respectivos controles de cambio en el plan de pruebas en caso de que sea requerido.	Grupo de seguridad de la información
60	**Ejecutar las pruebas** Divulgar el plan de pruebas a los administradores y demás personal requerido. El grupo de Seguridad de la Información notificará el inicio de las pruebas al personal encargado con el fin de que se realice el monitoreo de	Grupo de Seguridad de la Información, Contratista o tercero encargado de realizar las pruebas

ETAPA	ACTIVIDAD	RESPONSABLE
	disponibilidad de los activos de acuerdo con la afectación propuesta en el plan de pruebas. Esto debe incluir el tipo de prueba que se realizará, si es con usuario o sin usuario. Dependiendo del tipo de prueba se identificarán más o menos vulnerabilidades simulando escenarios reales en el que un atacante podría ejecutar una prueba similar. Debe identificarse adicionalmente si existen pruebas que afecten los servicios, con el fin de ejecutarlos de forma controlada. **Registro** Correo electrónico	
70	**Analizar la información documentar el informe** Una vez se cuente con los resultados entregados por las herramientas de vulnerabilidad, deberán llevarse a cabo las siguientes actividades: • Analizar cada una de las vulnerabilidades identificadas por dirección IP, activo y nivel de criticidad. • Descartar los falsos positivos de acuerdo con el sistema operativo, los sistemas de información instalados, las condiciones de explotación de las vulnerabilidades, entre otros. • Realizar comparaciones con los análisis que se hayan realizados anteriormente. • De acuerdo con los resultados identificados, se debe documentar el informe de resultados incluyendo la información de la vulnerabilidad, su descripción, su recomendación de solución, referencias, y nivel de severidad. De igual forma deben incluirse los hallazgos más significativos, activos con mayor cantidad de vulnerabilidades, vulnerabilidades por criticidad, por vector (externo, interno) o por ciudad, tiempos de remediación, conclusiones y recomendaciones. • Presentar o enviar los resultados al personal involucrado o responsable de los activos. **Registro**: Matriz de vulnerabilidades de la infraestructura tecnológica.	Grupo de seguridad de la información
80	**Revisar Informe** Revisar el informe entregado por el Grupo de Seguridad de la Información o Contratista Tercero y entregar comentarios para sus mejores.	Profesional Especializado Grado 6 - Seguridad informática
90	**Remediar las vulnerabilidades de acuerdo con el informe** • Una vez se hayan presentado los resultados, es responsabilidad de los administradores de los servicios tecnológicos revisar el detalle técnico de las vulnerabilidades identificadas, validar las acciones de remediación propuestas y definir una estrategia para la implementación de dichas acciones. Esto podría incluir: Remediación de vulnerabilidades por nivel de criticidad. • Instalación masiva de parches de seguridad. • Remediación de vulnerabilidades por tipo de aplicación. • Agrupación de los problemas de seguridad por tipo de activo. Por ejemplo: Sistemas operativos, software, aplicaciones web/cliente-servidor, bases de datos, equipos de red, seguridad, etc. Una vez seleccionada la estrategia de remediación se procederá a ejecutar la remediación correspondiente.	Administradores de las plataformas tecnológicas

ETAPA	ACTIVIDAD	RESPONSABLE
	Para los sistemas de información que sean críticos en la entidad se deben implementar las correcciones en ambiente de prueba como primera medida antes de desplegarlos en la infraestructura de producción. En caso de que surjan problemas al implementar las acciones de remediación, por ejemplo, que exista incompatibilidad con firmware o sistema operativo del equipo, se deberá informar al Profesional Especializado Grado 6 – Seguridad Informática, con el fin de que se tome la decisión de si se acepta la vulnerabilidad por un periodo acorado (no más de 1 año) o si se pueden implementar controles compensatorios **Registro:** Control de cambios	
100	**Realizar pruebas de verificación o Re-Test** Una vez se hayan implementado las acciones de remediación, se deben ejecutar estas pruebas con el objetivo de determinar si se llevó a cabo la implementación de forma correcta. El resultado del re-test no solo permite comprobar la corrección de las vulnerabilidades sino también identificar nuevas vulnerabilidades sobre los equipos. Estas últimas estarán sujetas al mismo procedimiento de clasificación, organización, socialización y remediación. La prueba de validación (re-test) se realiza únicamente a las vulnerabilidades que hayan sido remediadas en el periodo de corrección. Nota: El retest debe realizarse por lo menos una vez en el año. Registro: Matriz de vulnerabilidades de la infraestructura tecnológica	Grupo de seguridad de la información
110	**Seguimiento y monitoreo** Realizar un monitoreo y seguimiento al proceso de gestión de vulnerabilidades cada seis meses en cada una de sus etapas. Lo anterior para tener control del proceso y alimentar otros procesos internos como por ejemplo la Gestión de Incidentes o la Gestión de Riesgos de Seguridad de la Información **Registro:** Correo electrónico o acta de reunión	Profesional Especializado Grado 6 - Seguridad informática y Grupo de seguridad de la información
120	**Fin**	

8. TABLA DE FORMATOS

CÓDIGO	NOMBRE	UBICACIÓN	RESPONSABLE
R-DT-014	Matriz de vulnerabilidades de la infraestructura tecnológica	Intranet	Profesional Especializado Grado 06 Seguridad de la Información