

INFORME MENSUAL DE HERRAMIENTA MODULAR DEL SGSI – 2823-23

PERIODO: 24 DE SEPTIEMBRE A 23 DE OCTUBRE DE 2024



DOCUMENTO CONFIDENCIAL
Elaborado por:



Versión 1.0

OCTUBRE, 2024
Bogotá D.C

Historial de versiones

Id	Fecha (dd/mm/aa)	Versión	Descripción	Elaborado por	Revisado por
1	23/10/2024	1.0	Elaboración inicial del documento.	Password Consulting Services S.A. S	Gerencia de Proyecto

CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVO	3
3. ALCANCE	3
4. DEFINICIONES	3
5. ACTIVIDADES EJECUTADAS	4
6. EVIDENCIÁS DE ACTIVIDADES	12
7. CONCLUSIONES	19

1. INTRODUCCIÓN

El presente documento describe las actividades realizadas en el periodo del 24 de septiembre al 23 de octubre del año en curso, para dar cumplimiento al contrato 2823- 23 cuyo objeto es “contratar el mantenimiento y actualización de la herramienta modular de seguridad de la información”

2. OBJETIVO

Presentar los resultados obtenidos durante la ejecución de las actividades planeadas para el periodo del 24 de septiembre al 23 de octubre del año en curso, así como la atención de requerimientos de soporte y mantenimiento de la herramienta modular para la gestión del Sistema de Seguridad de la Información - GPSecure.

3. ALCANCE

Ejecución de las actividades planeadas para el contrato No. 2823- 23 con el objeto “contratar el mantenimiento y actualización de la herramienta modular de seguridad de la información”.

4. DEFINICIONES

El listado de términos relacionados a continuación, tienen como finalidad brindar un mayor entendimiento al contenido del documento:

- **SGSI:** Sistema de Gestión de Seguridad de la Información, es un conjunto de procesos para gestionar eficientemente la accesibilidad de la información en una organización; buscando asegurar los tres pilares confidencialidad, integridad y disponibilidad y minimizando a la vez los riesgos de seguridad de la misma (ISO/IEC 27001:2022).
- **Herramienta Modular:** Sistema de información compuesto por distintos módulos cuya funcionalidad permiten la asignación de roles y permisos

Código: F-PRO-23 Revisión N°: 1 Fecha: 03/01/2022 Página: 3

según la necesidad. (Definición propia, Password Consulting Services S.A.S, 2024).

- **Mantenimiento:** Hace referencia a los procedimientos preventivos y correctivos para que un sistema de información, aplicativo, o herramienta se encuentre en condiciones óptimas para su funcionamiento. (Definición propia, Password Consulting Services S.A.S, 2024).
- **Actualización:** Es el despliegue de una nueva versión que incluye más funcionalidades o corrige fallos de la versión precedente (Definición propia, Password Consulting Services S.A.S, 2024).

5. ACTIVIDADES EJECUTADAS

A continuación, se describen las actividades que se encuentran en ejecución en el periodo del 24 de septiembre al 23 de octubre del año en curso.

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
1	Matriz de riesgos	Recopilar y enviar la matriz de riesgos completa. Revisar y analizar todos los registros contenidos en la matriz de riesgos.	Transmilenio	24/08/2024	En progreso	Evidencia 1) evidenciaMR
2	Revisión documentos MSPI artículo 3. lineamientos generales	1) m-dt-001 políticas de seguridad y privacidad de la información. 2) m-dt-004 manual del sistema de gestión de seguridad de la información (sgsi) - resolución no. 355 del 2022	Password,	24/07/2024	Terminado	1. Es necesario que la Política y el Manual se actualicen a las versiones de la norma ISO 27001:2022. De acuerdo con lo establecido en la norma la política se debe actualizar como mínimo 1 vez al año (año de la última revisión 2022). 2. Se cuenta con la guía gestión de incidentes de seguridad digital, sin embargo, debe ajustarse e incluir mejoras debido a que el documento es muy antiguo (2020). 3. En los documentos del Manual y políticas de seguridad se mencionan lineamientos para los temas abordados, sin embargo. De acuerdo con lo establecido en la norma la política se debe actualizar como mínimo 1 vez al año (última revisión 2022). 4) evidencia1

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
3	Revisión documentos MSPI artículo 4. sistema de gestión de seguridad de la información y seguridad digital	1)m-dt-001 políticas de seguridad y privacidad de la información 2) m-dt-004 manual del sistema de gestión de seguridad de la información (sgsi) - resolución no. 355 del 2022	Password, Transmilenio	24/07/2024	Terminado	Es necesario que la Política y el Manual se actualicen a la versión de la norma ISO 27001:2022. De acuerdo con lo establecido en la norma la política se debe actualizar como mínimo 1 vez al año (última revisión 2022). 2) evidenciap
	Revisión documentos MSPI artículo 5. la estrategia de seguridad digital.	1) m-dt-001 políticas de seguridad y privacidad de la información 2) m-dt-004 manual del sistema de gestión de seguridad de la información (sgsi) 3) resolución no. 355 del 2022 4) t-dt-006 plan estratégico de seguridad de la información (pesi) 4) mapa de ruta de proyectos del pesi	Password, Transmilenio	24/07/2024	Terminado	1. De acuerdo con el Decreto 1083 de 2015: Artículo 2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año. Debe existir los siguientes planes: 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. 12. Plan de Seguridad y Privacidad de la Información. 2. En el momento que se establezca el Plan de Seguridad y Privacidad de la Información, se contemplará las actividades correspondientes a la protección de la información digital, medios impresos y físicos digitales y no digitales. 3. Mediante los lineamientos dados por Min TIC para la implementación de la estrategia de seguridad digital, se articula el Sistema de Gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; con el MSPI el cual contempla cinco (5) fases, las cuales

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
						<p>permiten que la Entidad pueda gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información.</p> <p>FASES:</p> <p>i. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.</p> <p>ii. Planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.</p> <p>iii. Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.</p> <p>iv. Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.</p> <p>v. Mejoramiento Continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.</p> <p>4. La entidad cuenta con el PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, sin embargo debe ajustarse e incluir mejoras debido a que el documento es muy antiguo (2020), además se debe contemplar los lineamientos establecidos en la Guía 21 - Gestión de Incidentes. En la documentación aportada por la entidad no se evidencia una guía de gestión de riesgos de seguridad de la información, sin embargo se evidencio el ANEXO 1 METODOLOGÍA PARA LA ADMINISTRACIÓN DE LOS</p>

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
						RIESGOS DE GESTIÓN. 5) evidenciae
	Revisión documentos MSPI artículo 6. la gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad	1) i-dt-001 instructivo para la identificación, valoración y clasificación de activos de información 2) m-dt-001 políticas de seguridad y privacidad de la información 3) m-dt-001 anexo 1 excepciones de seguridad de la información	Password, Transmilenio	24/07/2024	En progreso	
	revisión documentos MSPI artículo 7. operaciones seguras.	1) t-dt-13 protocolo de monitoreo de ciberseguridad 2) t-dt-003 protocolo a seguir para gestionar el uso de los medios removibles 3) p-dt-012 procedimiento para el intercambio seguro de información electrónica	Password, Transmilenio	24/07/2024	Terminado	T-DT-13 PROTOCOLO DE MONITOREO DE CIBERSEGURIDAD: El documento debe ser actualizado y enfocado a la versión de la norma ISO 27001:2022. T-DT-003 PROTOCOLO A SEGUIR PARA GESTIONAR EL USO DE LOS MEDIOS REMOVIBLES: Se cuenta con el documento, está incluida la norma ISO 27001:2022, como documento de referencia. * PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACIÓN ELECTRÓNICA: En la carpeta de los documentos compartidos no se evidencio el procedimiento. 1) evidenciaC
	Revisión documentos MSPI artículo 8. controles e interoperabilidad	n/a	Password, Transmilenio	24/07/2024	Terminado	Es necesario saber cuáles son los controles y procesos de la entidad que habilitan la integración al servicio, para lograr verificar la implementación de los mismos. Se debe hacer llegar los controles correspondientes. 1) evidenciaCP
	revisión documentos MSPI artículo 9. gestión de incidentes de seguridad digital	1) p-dt-020 procedimiento para la gestión de incidentes de seguridad de la información 2) t-dt-13 protocolo de monitoreo de ciberseguridad 3) t-dt-009 protocolo a seguir para el	Password, Transmilenio	24/07/2024	Terminado	PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 1. El procedimiento debe ajustarse e incluir mejoras debido a que el documento es muy antiguo (2020), además se debe contemplar los lineamientos establecidos en la Guía 21 - Gestión de Incidentes - Gobierno digital - MinTIC. 2. En el procedimiento existen los roles y

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
		contacto con las autoridades y grupos de interés especial encargadas de gestionar el sgsi				responsabilidades, sin embargo, se debe verificar si en la actualidad se está implementando los mismos. 3. No se observó evidencias del reporte de incidentes a través del formato de reporte de CSIRT. 4. No se observo 5) evidencialC
	Revisión documentos MSPI artículo 10. privacidad de la información.	1) m-sc-006 política de tratamiento y protección de datos personales. 2) m-dt-001 políticas de seguridad y privacidad de la información 3) resolución no. 355 del 2022	Password, Transmilenio	24/07/2024	Terminado	POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES: El documento cumple con las directrices correspondientes de acuerdo con lo estipulado en la normatividad aplicable, sin embargo, debería realizarse una nueva revisión y posible actualización frente a posibles cambios internos o mejoras que se consideren pertinentes. 1) evidencialD
	Revisión documentos MSPI artículo 11. mecanismos de autenticación.	1) m-dt-001 políticas de seguridad y privacidad de la información (numeral: 8.4.2 identificación y autenticación) 2) m-dt-002 manual para la administración de usuarios 3) p-dt-021 procedimiento de control de acceso físico	Password, Transmilenio	24/07/2024	Terminado	M-DT-001 POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (numeral: 8.4.2 Identificación y autenticación): Los lineamientos deben ser actualizados de acuerdo con la versión de la norma ISO 27001:2022. Se debe tener en cuenta que la norma indica que la política se debe actualizar como mínimo 1 vez al año (última revisión 2022). * M-DT-002 MANUAL PARA LA ADMINISTRACIÓN DE USUARIOS: El manual debe ajustarse e incluir mejoras debido a que el documento es muy antiguo (2020). Tener en cuenta la norma ISO 27001:2022 * P-DT-021 PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO: El procedimiento debe ajustarse e incluir mejoras de acuerdo con la realidad actual de la entidad. El documento es muy antiguo (2021). Tener en cuenta la norma ISO 27001:2022. 1) evidencialU
	Revisión documentos MSPI artículo 12. retención y destrucción	1) p-dt-019 procedimiento para realizar copias de respaldo y restauración de información 2) m-dt-001 políticas	Password, Transmilenio	24/07/2024	Terminado	El artículo 12 de la Resolución 500 de 2021 indica: RETENCIÓN Y DESTRUCCIÓN FINAL DE INFORMACIÓN. Los sujetos obligados deben establecer procesos y procedimientos para la retención y destrucción final de la información digital, para ello seguirán las

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
	final de información	de seguridad y privacidad de la información (numeral: 9.2.2.3 gestión de medios removibles) tablas de retención documental				<p>normas de gestión documental digital dispuestas por el Archivo General de la Nación.</p> <p>P-DT-019 PROCEDIMIENTO PARA REALIZAR COPIAS DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN: El procedimiento debe ajustarse e incluir mejoras debido a que el documento es muy antiguo (2020). Además, no especifica los lineamientos para la retención y destrucción final de la información digital. Es fundamental que la entidad cuenta con los lineamientos correspondientes para la atención y destrucción final de la información digital, teniendo en cuenta la normatividad archivística dispuesta por el Archivo General de la Nación, en este caso a Ley 594 de 2000 o Ley General de Archivo, dentro del cual se debe seguir el procedimiento establecido en el Artículo 15 del Acuerdo 04 de 2013, así: ARTÍCULO 15°. Eliminación de Documentos. La eliminación de documentos de archivo, tanto físicos como electrónicos, deberá estar basada en las tablas de retención documental o en las tablas de valoración documental, y deberá ser aprobada por el correspondiente Comité Institucional de Desarrollo Administrativo o el Comité Interno de Archivo según el caso. Se podrá elevar consulta al Archivo General de la Nación cuando no existan normas legales que regulen los plazos de retención de ciertos documentos; a su vez éste podrá solicitar concepto al organismo cabeza de sector al que corresponda la documentación objeto de consulta. Adicionalmente se deberá cumplir con el siguiente procedimiento.</p> <p>i. Previamente y por un periodo de treinta (30) días se deberá publicar en la página Web de la respectiva entidad, el inventario de los documentos que han cumplido su tiempo de retención y que en consecuencia pueden ser eliminados, de forma que los ciudadanos puedan enviar sus observaciones sobre este proceso, a los Consejos Departamentales y Distritales de Archivos o al Archivo General de la Nación.</p> <p>ii. Las observaciones deberán ser revisadas por el respectivo Consejo Departamental y Distrital de Archivos o el Archivo General de la Nación, para lo cual contarán con sesenta (60) días, instancia que con base en el fundamento presentado por el o los peticionarios, podrá solicitar a la entidad</p>

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
						<p>suspender el proceso de eliminación y ampliar el plazo de retención de los documentos. Todo lo anterior se hará público en los sitios Web de la entidad.</p> <p>iii. La aprobación de la eliminación de documentos de archivo, tanto en soporte físico como electrónico, deberá constar en un Acta de Eliminación de Documentos, la cual suscribirán el presidente y secretario técnico del Comité Institucional de Desarrollo Administrativo o el Comité Interno de Archivo según el caso, de la respectiva entidad.</p> <p>iv. Las actas de eliminación y el inventario de los documentos que han sido eliminados, se conservarán permanentemente y la entidad deberá mantenerlos publicados en su página Web para su consulta.</p> <p>v. El Archivo General de la Nación será la última instancia en cuanto a las solicitudes de suspensión de los procesos de eliminación, de acuerdo con la naturaleza de los documentos y su valor legal, testimonial, informativo, cultural, histórico o científico, cuando a su juicio se pueda afectar el patrimonio documental del país.</p> <p>vi. La eliminación de documentos se debe llevar a cabo por series y subseries documentales y no por tipos documentales. Por ningún motivo se pueden eliminar documentos individuales de un expediente o una serie, excepto que se trate de copias idénticas, o duplicados.”</p> <p>1) evidencialR</p>
	Revisión documentos MSPI artículo 13. seguridad digital desde el proceso de desarrollo de software	1)t-dt-002 protocolo estándares para el desarrollo de software en Transmilenio s. a 2) m-dt-001 políticas de seguridad y privacidad de la información (numeral: 9.4 política de desarrollo seguro). matriz de seguridad para desarrollo seguro	Password, Transmilenio	24/07/2024	Terminado	<p>* T-DT-002 PROTOCOLO ESTANDARES PARA EL DESARROLLO DE SOFTWARE EN TRANSMILENIO S.A: El documento debe ser actualizado fue creado en el 2017, teniendo en cuenta Ley 1581 de 2012, el Decreto 1074 de 2015 y la norma ISO 27001:2022.</p> <p>* M-DT-001 POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (numeral: 9.4 POLÍTICA DE DESARROLLO SEGURO): Los lineamientos deben ser actualizados de acuerdo con la versión de la norma ISO 27001:2022. Se debe tener en cuenta que la norma indica que la política se debe actualizar como mínimo 1 vez al año (última revisión 2022).</p> <p>1) evidenciaDs</p>

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
	Revisión documentos MSPI artículo 14. terceros, colaboradores y seguridad digital	1) plan de auditoría de proveedores checklist de seguridad proveedores 2) m-dt-001 políticas de seguridad y privacidad de la información (numeral de gestión de proveedores)	Password, Transmilenio	24/07/2024	Terminado	Los siguientes documentos no se encontraron en la carpeta de evidencias: - Plan de auditoría de proveedores. - Checklist de seguridad proveedores. M-DT-001 POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (numeral de gestión de proveedores): Política de seguridad de la información para las relaciones con los proveedores, el documento cumple con las directrices correspondientes de acuerdo con lo estipulado en la normatividad aplicable, sin embargo debería realizarse una nueva revisión y posible actualización frente a posibles cambios internos o mejoras que se consideren pertinentes. Además de acuerdo con lo establecido en la norma la política se debe actualizar como mínimo 1 vez al año (año de la última revisión 2022). 1) evidenciaCL
	Revisión documentos MSPI artículo 15. control de las actividades incluidas en la estrategia de seguridad digital y gestión de riesgos	1 y 2. plan de auditoría de control interno. 3. indicador nasi	Password, Transmilenio	24/07/2024	Terminado	Los siguientes documentos no se encontraron en la carpeta de evidencias: 1 y 2. Plan de auditoría de Control Interno. 3. Indicador NASI. De acuerdo con lo anterior no es posible realizar la verificación documental y lo indicado en la columna H.
	Revisión documentos MSPI artículo 16. seguridad digital y responsabilidad	1) manual de riesgos matriz de riesgos tic presentación de pólizas	Password, Transmilenio	24/07/2024	Terminado	Los siguientes documentos no se encontraron en la carpeta de evidencias: *M-OP-002 Manual para la gestión del riesgo en TRANSMILENIO S.A". *Matriz de riesgos TIC. * Presentación de Pólizas.
	Revisión documentos MSPI artículo 17. etapas generales de	1)p-dt-020 procedimiento para la gestión de incidentes de seguridad de la información 2) t-dt-13 protocolo de monitoreo de	Password, Transmilenio	24/07/2024	Terminado	T-DT-13 PROTOCOLO DE MONITOREO DE CIBERSEGURIDAD: El documento debe ser actualizado y alineado a la versión de la norma ISO 27001:2022. 1) evidenciaCS

N.	Actividad	Descripción	Responsable	Inicio	Fin	Observaciones
	la gestión de incidentes de seguridad digital	ciberseguridad				

6. EVIDENCIÁS DE ACTIVIDADES

Las evidencias comprenden registros detallados de las actividades realizadas por el equipo de password durante el período del 24 de agosto al 23 de septiembre.

- Matriz de riesgos.



Imagen (1): evidenciaMR

- Revisión documentos gestión de riesgo.

	TÍTULO: PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
	Código: P-DT-020	Versión: 0	Fecha: Diciembre de 2020	

TABLA DE CONTENIDO

1.	OBJETO	2
2.	ALCANCE	2
3.	RESPONSABLE	2
4.	DOCUMENTOS DE REFERENCIA	2
5.	DEFINICIONES	3
6.	CONDICIONES GENERALES	4
6.1	Roles y responsabilidades de la gestión de incidentes	4
7.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	6
7.1	Identificación y reporte de eventos	6
7.2	Registro de eventos	7
7.3	Evaluación de eventos y declaración de incidentes	8
7.4	Clasificación de incidentes	9
7.5	Priorización de incidentes	9
7.6	Escalamiento de incidentes	11
7.7	Tratamiento de los incidentes	12
7.8	Recolectar y analizar la evidencia del incidente	13
7.9.	Procedimiento forense	13
7.10	Medidas Disciplinarias	14

Imagen (2): evidencia

- Políticas

	TÍTULO: POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	Código: M-DT-001	Versión: 6	Fecha: Diciembre 2022	

- Borrado Seguro: Aplica solo para medio magnéticos, es un borrado a bajo nivel.
- Trituración: Esto aplica más que todo a la destrucción de papel por medio de máquinas trituradoras.

Dependencia: oficina o área de la entidad.

Directorio activo: es un repositorio que contiene información sobre las propiedades y la ubicación de los diferentes tipos de recursos dentro de la red distribuida de una empresa.

Dominio: Áreas en las que se desarrolla la NTC/ISO 27001.

Disponibilidad: es la característica o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Imagen (3): evidenciap

- Plan estratégico

repetible y efectivo.

6.3. Definición de iniciativas de seguridad de la información

Teniendo en cuenta el resultado anterior, se identificaron las iniciativas de seguridad de la información, las cuales se encuentran alineadas con el Plan Estratégico Institucional y con los resultados de la calificación obtenida en el autodiagnóstico del MSPI presentado anteriormente en la situación actual. Es importante aclarar que las iniciativas están enmarcadas dentro de los controles de seguridad sugeridos para garantizar una adecuada arquitectura de seguridad de la información y un esquema de defensa a profundidad utilizando soluciones y tendencias de seguridad de la información y de tecnología. Estas iniciativas fueron seleccionadas de acuerdo con el nivel de madurez de cada Dominio teniendo como referencia la calificación actual obtenida 65%.

De igual forma, los objetivos estratégicos de seguridad de la información que se desean cumplir a través del PESI son:

- **Gobierno o Modelo de seguridad de información:** lograr desplegar un modelo de

Imagen (4): evidenciae

- Protocolos

1. OBJETO

Establecer las acciones y conductas a seguir para llevar a cabo el proceso de monitoreo de ciberseguridad en la infraestructura tecnológica de TRANSMILENIO S.A.

2. ALCANCE

El presente protocolo se aplica en la revisión y seguimiento de la información obtenida a partir de las herramientas de seguridad empleadas para la detección de ataques y/o comportamientos anómalos al interior de **TRANSMILENIO S.A.**

Este protocolo aplica el grupo de seguridad de la información de la Dirección de TIC

3. RESPONSABLE

El responsable de la elaboración y/o actualización de este protocolo es el Profesional Especializado Grado 6 - Seguridad Informática, de la Dirección de TIC. De igual forma, el Director de TIC velará por el estricto cumplimiento, implementación y mantenimiento de este protocolo.

La revisión y/o actualización de este protocolo deberá realizarse cuando se considere pertinente por parte de los responsables de su actualización.

Imagen (5): evidenciaC

- Controles

A.5	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	72	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	59	100	EFFECTIVO
A.9	CONTROL DE ACCESO	66	100	GESTIONADO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	72	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	69	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	63	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	46	100	EFFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	63	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	EFFECTIVO
A.18	CUMPLIMIENTO	76	100	GESTIONADO

Imagen (6): evidenciaCP

- Incidentes

Al presentarse un evento de seguridad sobre un equipo de cómputo, se deben tener en cuenta las siguientes condiciones:

- No reiniciar el equipo.
- No apagar el equipo.
- No conectar ni desconectar el cable de red del equipo
- Informar sobre los eventos ocurridos de forma inmediata.
- Hacer fotografías de mensajes o errores de sistema mostrados en pantalla.

Por otro lado, los siguientes componentes son fuentes generadoras de eventos de seguridad de la información:

- Alarmas en la infraestructura
- Alertas en sistemas de seguridad
- Fallas en la disponibilidad de servidores
- Logs de servidores, equipos de red, aplicaciones y herramientas de seguridad
- Resultados de pruebas de vulnerabilidad y hacking ético.

7.2 Registro de eventos

Todos los eventos deberán quedar registrados luego de ser reportados. Este registro del evento se debe realizar por el Grupo de Seguridad de la Información en la herramienta dispuesta para tal fin.

Imagen (6): evidenciaIC

- Datos personales

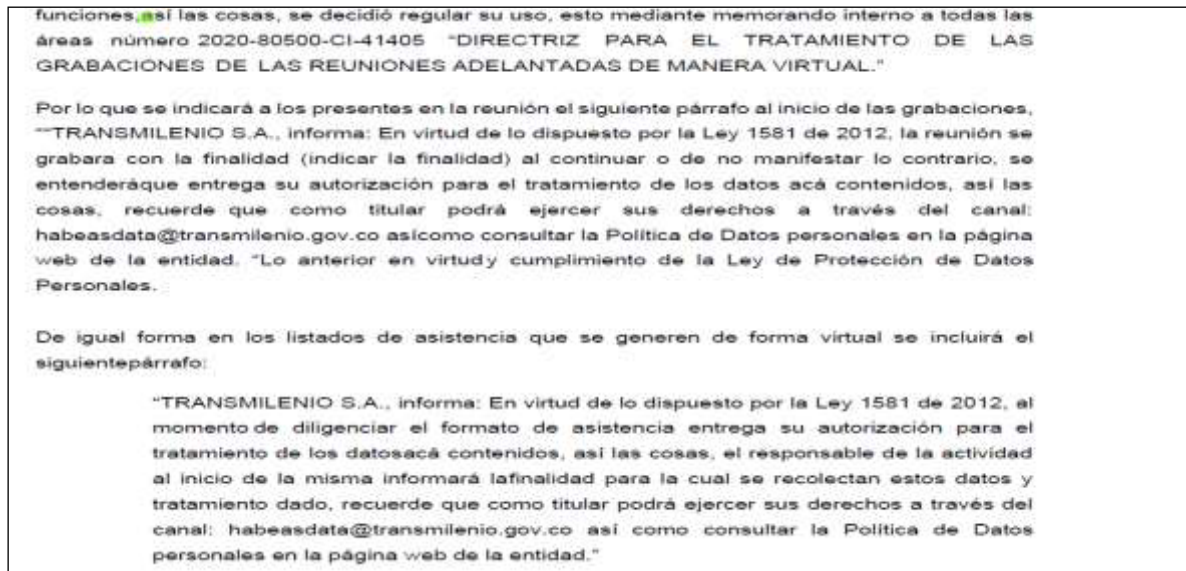


Imagen (7): evidenciaD

- Manual para la administración de usuarios

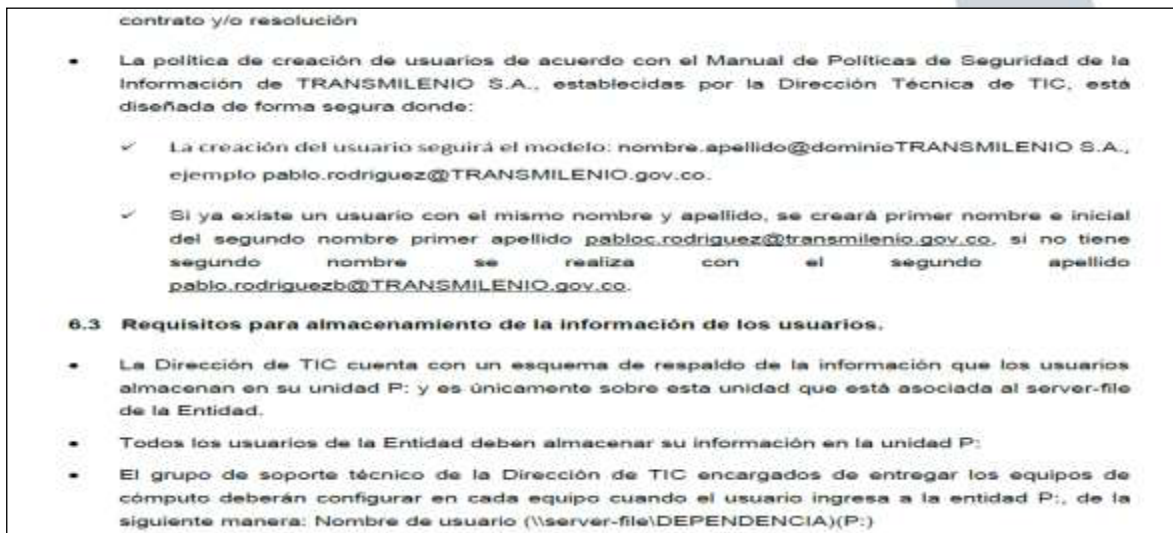


Imagen (8): evidenciaU

- Copias de respaldo

7. DESCRIPCIÓN DE ACTIVIDADES		
7.1 Copias de respaldo		
7.1.1 Respaldo de la información de Usuarios		
A continuación, se describen los pasos que se deben seguir para realizar el respaldo de la información de los usuarios, almacenada en la unidad (P:).		
ETAPA	ACTIVIDAD	RESPONSABLE
10	Inicio	
20	Almacenar los archivos en la unidad P:\	Usuarios de TMSA
30	Configurar la(s) herramienta(s) de respaldo para que realice la copia de la Unidad P: en cinta. Esta configuración se realiza de tal forma que la copia de respaldo se inicie automáticamente.	Técnico Administrativo Grado 02 - Soporte a Infraestructura de TIC's y Mesa de Ayuda
40	Insertar en el equipo de respaldo las cintas etiquetadas con su respectivo código de barras y previamente configuradas, esto se realiza antes de que inicie la copia de respaldo. En estas cintas se almacenarán los datos respaldados de cada uno de los usuarios.	Técnico Administrativo Grado 02 - Soporte a Infraestructura de TIC's y Mesa de Ayuda

Imagen (9): evidenciaR

- Desarrollo de software

7. ESTÁNDARES PARA EL DESARROLLO DE SOFTWARE EN TRANSMILENIO S.A.
7.1. Estándares generales aplicables a todo tipo de sistemas para el uso del repositorio de versiones
<p>Todo desarrollo debe registrarse en el repositorio de versiones del código institucional.</p> <p>Toda actualización al repositorio (update/ commit) debe ir precedida de una operación de actualización del área de trabajo local (pull/ update).</p> <p>Toda actualización al repositorio debe haber sido probada de antemano.</p> <p>Toda línea nueva de desarrollo realizada sobre el código existente debe realizarse como una nueva rama del proyecto en el repositorio.</p> <p>Se debe incluir, al momento de actualizar algún artefacto en el repositorio, un breve comentario con la justificación de dicha actualización.</p>
1.1. Comunicación

- Imagen (10): evidenciaDe

- Check list

7.1 REQUISITOS DE VALIDACION DE ENTRADA.			
LINEAMIENTOS	APLICA (SI/NO)	IMPLEMENTADO (SI/NO)	DESCRIPCION DE COMO SE IMPLEMENTA O JUSTIFICACION DE NO ESTAR IMPLEMENTADO
Se deberán cumplir con los siguientes requisitos de validación de entrada en formularios, campos o cualquier punto de inserción de datos de entrada en las aplicaciones.			
7.1.1. Toda validación de datos se deberá realizar del lado del servidor o punto confiable, nunca de forma local o scripts en el navegador.	SI	SI	Programación web
7.1.2. Todas las fuentes de datos deberán identificarse y clasificarse en confiables y no confiables. De igual forma, cuando se usen fuentes de datos que no sean confiables, entonces se deberá realizar su respectiva validación antes de ser procesados (por ejemplo, bases de datos, secuencias de archivos, etc.)	NO	NO	Responsabilidad de TMSA
7.1.3. En el caso que sea posible se deberá construir una rutina de validación de entrada controlada para la aplicación.	SI	SI	Cada modelo tiene su validación propia y la global dependiendo de la interfaz que implementa
- Se deben especificar conjuntos de caracteres adecuados, como UTF-8, para todas las fuentes de entrada.	NO	NO	No aplica en Tdoc
- Se deberán codificar los datos en un conjunto de caracteres común antes de validarlos (Caracterización).	NO	NO	No aplica en Tdoc
- Todas las fases de validación de los datos de entrada deberán resultar en el rechazo de la entrada.	SI	SI	Se modifica el ModelState para añadir los errores
7.1.4. Si el sistema admite juegos de caracteres extendidos UTF-8 estos se deberán validar después de que se complete la decodificación UTF-8.	NO	NO	No aplica en Tdoc
7.1.5. Se deben validar todos los datos proporcionados por el cliente antes de procesarlos, esto incluye todos los parámetros, las URL y el contenido del encabezado HTTP (por ejemplo, nombres y valores de cookies). Se deben incluir en esta práctica también las respuestas automáticas de JavaScript, Flash u otro código embebido.	SI	SI	Cada modelo tiene su validación propia y la global dependiendo de la interfaz que implementa. Además se codifica cualquier carácter que pueda causar inyección de código malicioso
7.1.6. Se deberá verificar que los valores de los encabezados en las solicitudes (Request) y respuestas (response) contengan solo caracteres ASCII.	SI	SI	Tecnología
7.1.7. Los datos de las redirecciones deben validarse (un atacante puede enviar contenido malicioso directamente al objeto de la redirección, evitando así la lógica de la aplicación y cualquier validación realizada antes de la redirección).	SI	SI	Validación y prevención por tecnología
7.1.8. Siempre se deberá validar:			
- Los tipos de datos esperados por la aplicación.	SI	SI	Criterio parametrizables
- Rango de datos.			
- Longitud de datos.			
7.1.9. Las entradas deberán ser validadas a través de una lista "blanca" de caracteres permitidos, siempre	SI	SI	Configuración RBM

- Imagen (11): evidenciaCI

- Ciber seguridad

6.1 Roles de monitoreo de ciberseguridad

El equipo de monitoreo de ciberseguridad definido para llevar a cabo el desarrollo de las respectivas reuniones de monitoreo, estará conformado por los roles participantes que se describen en este capítulo. Se aclara que los participantes que asisten a las reuniones serán aquellos requeridos según los aspectos objeto de monitoreo. Por lo anterior, es posible que en alguna de las reuniones se pueda convocar a otros colaboradores o proveedores de la Entidad.

Las reuniones de monitoreo de ciberseguridad serán lideradas por el Profesional Especializado grado 6 – Seguridad informática y el Profesional Especializado grado 6 – Coordinador de procesos corporativos

- **Rol Grupo de seguridad de la información:**
 - Administrador de Seguridad, Redes y comunicaciones
 - Contratistas de Seguridad de la Información
- **Rol Grupo de infraestructura tecnológica**
 - Administrador del directorio activo
 - Administrador de servidores

- Imagen (12): evidenciaCS

7. CONCLUSIONES

A la fecha de elaboración de este informe, no se presenta la materialización de riesgos de operación o de Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad); como tampoco se presenta una desviación negativa en las actividades planeadas.