Informe de gestión trimestra

Plan de Tratamiento de Riesgos de Seguridad en la informació

Cuarto Trimestre de 2023
Presentado Diciembre 21 de 2023

Introducción

Un riesgo de seguridad digital se conoce como un conjunto de amenazas y vulnerabilidades derivadas del entorno digital y que pueden comprometer la confidencialidad, integridad y su disponibilidad de los activos de información, afectando el logro de los objetivos institucionales, por tanto es importante realizar una identificación oportuna de posibles riesgos, así como el establecimiento de controles que permitan su mitigación.

En tal sentido, la USPEC definió la "Política de Administración de Riesgos" incluyendo lineamientos establecidos por el DAFP a través de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas". Esta guía definió los requisitos para la administración de riesgos de gestión, corrupción y seguridad digital a través de la identificación, análisis, valoración, tratamiento y seguimiento de aquellas acciones que permitirán mitigar los riesgos. Ahora bien, durante el primer trimestre se trabajó de manera integrada entre la Oficina de Tecnología y los diferentes procesos institucionales con el fin de actualizar las matrices de riesgos de seguridad digital, así mismo se definieron planes de tratamiento de riesgos con el fin de mitigar las vulnerabilidades detectadas.

1. SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS POR PROCESO

A continuación se presenta el avance de la ejecución del plan de tratamiento de riesgos de seguridad de información del proceso Gestión de Tecnologías de la Información.

Actividad	Responsable	Soporte	Fecha	Seguimiento 1 Trimestre
Riesgo: Posibilidad de pérdida de disponibilidad por fallas en el suministro del fluido eléctrico debido a la falta de mantenimiento de los componentes de la infraestructura tecnológica				
Actualizar el plan de mantenimiento de la plataforma tecnológica	Jefe Oficina de Tecnología	Plan de mantenimiento actualizado y socializado	15-01-2023 al 30-03-2023	**Avance de la actividad:** Actividad cumplida en el tercer trimestre **Ejecución del control:** Se realizaron los mantenimientos programados para el trimestre dentro de los cuales se encuentran aire acondicionado y UPS, sin embargo por parte de la OTEC no se llevó a cabo el respectivo seguimiento.
Realizar seguimiento semestral al plan de mantenimiento de la plataforma tecnológica	Administradores de plataforma tecnológica	Seguimiento al plan de mantenimiento con la gestión del trimestre	01-04-2023 al 31-12-2023	Se realizaron los mantenimientos programados para el trimestre dentro de los cuales se encuentran aire acondicionado y UPS, sin embargo por parte de la OTEC no se llevó a cabo el respectivo seguimiento.
Riesgo: Posibilidad de pérdida de disponibilidad por cambios sin autorización en los servicios que componen la plataforma tecnológica debido a la falta de gestión por parte de la supervisión de apoyo a los proveedores de TI				
Definir a través de un documento de apoyo de la OTEC, los lineamientos para llevar a cabo la gestión de proveedores de TI (Este documento será parte de la operación de TI por lo tanto no se formalizará dentro de la documentación de MIPGESTION)	Jefe Oficina de Tecnología	Documento de apoyo aprobado y socializado	01-02-2023 al 31-03-2023	**Avance actividad:** La actividad se culminó en el segundo trimestre **Ejecución control:** Los Supervisor de apoyo de los diferentes servicios han validado los cambios realizados en la plataforma tecnológica y servicios de TI por parte de los proveedores o de los administradores de la infraestructura tecnológica a través de la gestión del formato TI-PR-013 control de cambios, registrando los resultados de la actividad, para cada uno de los cambios mencionados anteriormente.
Realizar seguimiento al diligenciamiento del formato TI-PR-013 control de cambios	Encargado de SGSI	Soportes formato control de cambios	15-01-2023 al 31-12-2023	**Avance de la actividad**: De acuerdo al seguimiento realizado, durante el trimestre se realizó el siguiente control de cambios: * Instalación del certificado digital del software MIPGESTION **Ejecución control:** Los Supervisor de apoyo de los diferentes servicios han validado los cambios realizados en la plataforma tecnológica y servicios de TI por parte de los proveedores o de los

				administradores de la infraestructura tecnológica a través de la gestión del formato TI-PR-013 control de cambios, registrando los resultados de la actividad, para cada uno de los cambios mencionados anteriormente.
Riesgo: Posibilidad de pérdida de disponibilidad por interrupción en la operación de los servicios de TI debido a que no se realiza una adecuada gestión de la capacidad y las vulnerabilidades de la plataforma tecnológica				
Realizar seguimiento trimestral al estado de la plataforma de TI de acuerdo a los umbrales de gestión de la capacidad	Administradores de plataforma tecnológica	Informe de gestión de la capacidad con el análisis del trimestre	15-01-2023 al 31-12-2023	**Avance de la actividad y gestión del control:** Se realizó seguimiento trimestral al estado de la plataforma de TI de acuerdo a los umbrales de gestión de la capacidad. En términos generales se identificaron 8 alertas sobre los componentes de la infraestructura tecnológica. Al respecto se tomaron las acciones pertinentes por parte de los administradores de la plataforma tecnológica con el propósito de mitigar los posibles efectos. **Ejecución del control:** Los administradores de la plataforma tecnológica monitorean los componentes de la plataforma tecnológica a través de la revisión de los umbrales definidos en el instructivo A3-IN-02 Lineamientos técnicos para gestionar la capacidad de TI y registran de manera trimestral los resultados en el informe de gestión de la capacidad.
Definir a través de un método de operación los lineamientos de gestión de vulnerabilidades de la plataforma tecnológica	Administradores de plataforma tecnológica Encargado de Seguridad de Información	Método de operación aprobado, publicado y socializado	01-02-2023 al 31-03-2023	**Avance de la actividad:** La actividad referente al método de operación se cumplió en el primer trimestre. La actividad relacionada con el seguimiento al plan de remediación de vulnerabilidades no se pudo ejecutar teniendo en cuenta las siguientes consideraciones. Durante el cuarto trimestre del 2023 se llevó a cabo la gestión para realizar pruebas de vulnerabilidades a 5 sitios web de la USPEC dentro de los cuales se encuentran: INFODOC, Portal web, Intranet, Humano, Inventarios; labor que estuvo a cargo del CSIRT de Gobierno. Como resultado de este análisis se generaron un total de 54 vulnerabilidades catalogadas como medias (29) y bajas (25) las cuales se planean remediar en el 2024. Teniendo en cuenta que el informe de vulnerabilidades se recibió el 23 de noviembre de 2023, no se contó con el tiempo necesario para realizar el plan de remediación de vulnerabilidades. Este es la fuente principal para la ejecución del control. Por lo anterior, no fue posible generar de manera oportuna el plan de remediación de vulnerabilidades y por tanto no se contó con el insumo necesario para ejecutar el control propuesto.
Realizar seguimiento al plan de remediación de vulnerabilidades	Coordinador del Grupo de Comunicaciones	Seguimiento del plan de remediación de vulnerabilidades con la gestión realizada durante el trimestre	01-07-2023 al 31-12-2023	
Definir el cronograma de actualización de documentos de operación de la plataforma tecnológica	Administradores de plataforma tecnológica Encargado de Seguridad de Información	Cronograma definido	01-02-2023 al 31-03-2023	**Avance de la actividad:** Actividad cumplida en el primer trimestre. **Ejecución del control**: El encargado del SGSI validó la actualización de documentos de operación de TI a través de la revisión del cronograma establecido con los administradores de la plataforma tecnológica. Se elaboró un documento y el seguimiento se registró en las casillas de seguimiento del mismo cronograma.
Realizar seguimiento trimestral a la ejecución del cronograma de actualización de documentos de operación de la plataforma tecnológica	Encargado de Seguridad de Información	Cronograma con seguimiento de la gestión realizada durante el trimestre	01-04-2023 al 15-12-2023	**Avance de la actividad:** Se realizó seguimiento al cumplimiento del cronograma a través del cual se establecen los documentos de operación de la plataforma tecnológica. En conclusión durante el cuarto trimestre se elaboró un documento relacionado con la configuración del backup. **Ejecución del control:** El encargado del SGSI

				validó la actualización de documentos de operación de TI a través de la revisión del cronograma establecido con los administradores de la plataforma tecnológica. Se elaboró un documento y el seguimiento se registró en las casillas de seguimiento del mismo cronograma.
Riesgo: Posibilidad de pérdida de confidencialidad, integridad y disponibilidad por fuga de información debido a la falta de gestión sobre los documentos electrónicos				
Definir cronograma de implementación de controles para evitar fuga de información	Jefe Oficina de Tecnología	Cronograma definido	01-02-2023 al 31-03-2023	**Avance de la actividad:** Actividad cumplida en el primer trimestre. **Ejecución del control:** El Coordinador del Grupo de Comunicaciones verificó el cumplimiento de la ejecución de controles a través de la revisión del cronograma que contiene el listado de controles técnicos definidos con el fin de evitar la fuga de información institucional desde el servicio de nube del correo y del servidor de archivos, registrando el avance en la columna del seguimiento del cronograma.
Realizar seguimiento a cronograma	Jefe Oficina de Tecnología	Cronograma con seguimiento de la gestión realizada durante el trimestre	01-04-2023 al 15-12-2023	**Avance de la actividad:** Se realizó seguimiento al cumplimiento del cronograma a través del cual se establecen los controles para mitigar la fuga de información. En conclusión durante el segundo trimestre se ejecutaron las siguientes actividades: - Se avanzó en la actualización de la política de configuración de copias de respaldo, sin embargo de acuerdo a la revisión realizada con la Oficina Asesora Jurídica se hace necesario tomar decisiones al nivel del comité directivo, por el tiempo que requiere la gestión se pospone la actividad para la próxima vigencia. - Se reporta actividad ejecutada en el mes de agosto con la unificación de credenciales del usuario de red, correo institucional e intranet. No fue posible culminar la actividad relacionada con la habilitación el Single Sign On del correo institucional, teniendo en cuenta que a la fecha el proveedor del servicio de internet, no ha logrado configurar los DNS para darle salida al correo mediante este SSO, por tanto se pospone la actividad para la siguiente vigencia. **Ejecución del control:** El Coordinador del Grupo de Comunicaciones verificó el cumplimiento de la ejecución de controles a través de la revisión del cronograma que contiene el listado de controles técnicos definidos con el fin de evitar la fuga de información institucional desde el servicio de nube del correo y del servidor de archivos, registrando el avance en la columna del seguimiento del cronograma.

Revisó / Aprobó: Imelda Muñoz Mancipe
Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal
Profesional Especializado