Informe de gestión trimestral

Plan de Tratamiento de Riesgos de Seguridad en la información

Tercer Trimestre de 2022
Presentado Octubre 12 de 2022

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 por cada uno de los procesos institucionales, en él se relacionan los riesgos de cada proceso, las actividades propuestas y las gestiones realizadas durante el primer trimestre, posteriormente se encuentran las observaciones de la segunda línea de defensa, que para el caso de seguridad de información corresponde a la Oficina de Tecnología.

1.1 Proceso de gestión contractual

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de disponibilidad de las compras realizadas a través de la plataforma de Tienda Virtual	Actualizar el procedimiento Adquisiciones Tienda Virtual del Estado Colombiano estableciendo controles para centralizar la información de las compras realizadas por Tienda Virtual.	No se reportaron avances por parte del proceso. **Porcentaje de avance trimestre: 0%**

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ Se recomienda iniciar la gestión por parte de la Dirección de Gestión Contractual para llevar a cabo la actualización del procedimiento Adquisiciones Tienda Virtual del Estado Colombiano, con el fin de avanzar en la implementación de los controles propuestos y así mismo mitigar el riesgo de ¨Pérdida de disponibilidad de las compras realizadas a través de la plataforma de Tienda virtual¨.
- ✓ Porcentaje de avance del 3 trimestre: 0%.
- ✓ Porcentaje acumulado 2022: 0%

1.2 Proceso de gestión de infraestructura

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Fuga de información institucional por el uso de equipos portátiles personales	Socializar el lineamiento para el uso de portátiles y verificar que se está dando estricto cumplimiento al mismo, de acuerdo a las necesidades de la Dirección de Infraestructura.	Por parte de la Oficina de Tecnología se reiteró al Grupo Administrativo la solicitud de revisión de la propuesta actualizada de la circular que contiene los lineamientos para el uso de portátiles en la Entidad, sin embargo con corte al 30 de septiembre no se obtuvo respuesta. Una vez se cuente con el documento formalizado se procederá con su divulgación al personal de la Entidad y especialmente a la Dirección de Infraestructura para su implementación. **Porcentaje trimestre: 0%**

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de continuidad en la operación del proceso	Actualizar lineamientos para la verificación del cargue de información de las gestiones adelantadas por el personal de la Dirección de Infraestructura en la carpeta compartida, a través de un método de operación establecido por la Entidad.	Teniendo en cuenta el Memorando I-2022-000673 del 21 de febrero de 2022, los funcionarios de la DINFRA organizan la información en la carpeta compartida de la dirección de infraestructura según estructura descrita. Actualmente teniendo en cuenta la situación de trabajo de alternancia los funcionarios tienen acceso VPN tendiendo acceso a la carpeta compartida de la DINFRA, dicha información es verificada por el supervisor del contratista o persona designada según lo descrito en los informes mensuales quien verifica el almacenamiento de información y avala el informe para pago. Como soporte se anexa correo electrónico socializando la directriz al grupo DINFRA , informe mensual con enlaces, y una vez se firma contrato se anexa el acta de compromiso la cual contempla "Que en concordancia con el Sistema de Gestión de Seguridad de la Información el cual se implementó en USPEC de acuerdo con lo estipulado en el decreto 1078 de 2015, donde se establece, entre otras disposiciones los lineamientos generales de la Estrategia Gobierno en Línea, dentro de la cual se encuentra el componente número 4 que se refiere a Seguridad y Privacidad de la información de acuerdo con lo señalado en el artículo 5 del referido decreto y de acuerdo con la Política General de Seguridad de la Información de USPEC, Resolución 000181 del 2022". Se anexa como soporte actas de compromiso. **Porcentaje trimestre: 10%**

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de confidencialidad de los planos de los ERONES	Actualizar la directriz para el manejo de planos institucionales incluyendo lineamientos para el acceso de personal externo de la Entidad, y documentar en un método de operación.	El control de la entrega de planos físicos para consulta de acuerdo Directriz préstamo yo consulta de planos de la DINFRA, s debe ser consignado en el formato IN-FO-019. El soporte de los formatos diligenciados y aprobados se encuentra en la carpeta compartida de la DINFRA. Se anexa soporte formato actualizado préstamo yo consulta de planos y formato diligenciado de acuerdo a directriz. La directriz se encuentra consignada en formato actualizado y el cual se encuentra en MIPG. **Porcentaje trimestre: 10%**

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ Se recomienda continuar con la formalización de los lineamientos para el uso de portátiles y determinar los casos en que se requiere el uso de portátiles tanto personales como propios de la Entidad por parte del personal de la Dirección de Infraestructura, con el fin implementar el control propuesto y mitigar el riesgo.
- ✓ De acuerdo a los soportes revisados, es evidente la aplicación del control propuesto por la DINFRA para la verificación del cargue de información gestionada por parte de su personal. Sin embargo, de acuerdo a lo establecido en el plan de tratamiento no se evidencia la gestión para la formalización de las directrices a través de un método de operación de acuerdo a la actividad definida como tratamiento de riesgo.
- ✓ De acuerdo a los soportes revisados, es evidente la aplicación del control propuesto por la DINFRA para el manejo de planos institucionales. Sin embargo, de acuerdo a lo establecido en el plan de tratamiento no se evidencia la gestión para la formalización de las directrices a través de un método de operación de acuerdo a la actividad definida como tratamiento de riesgo.
- ✓ Porcentaje de avance del 3 trimestre: 7%.
- ✓ Porcentaje acumulado 2022: 30%

1.3 Proceso gestión de suministro de bienes y prestación de servicios

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de confidencialidad, integridad y disponibilidad de la información	Formalizar el lineamiento para la transferencia y consulta de información del listado censal a través de un método de operación definido por la Entidad.	No se reportaron avances por parte del proceso. **Porcentaje de avance trimestre: 0%**
	Realizar seguimiento al cumplimiento del lineamiento establecido.	No se reportaron avances por parte del proceso. **Porcentaje trimestre: 0%**

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ Se recomienda iniciar la gestión por parte de la Dirección Logística para llevar a cabo la formalización a través de un método de operación de los lineamientos para la transferencia y consulta del listado de información censal, con el fin de darle trascendencia y trazabilidad a las decisiones que se establecen desde la respectiva Dirección para el manejo de este tipo de información sensible y de esta manera avanzar en la implementación de los controles propuestos y así mismo mitigar el riesgo de ¨Pérdida de confidencialidad, integridad y disponibilidad de la información
- ✓ Porcentaje de avance del 3 trimestre: 0%.
- ✓ Porcentaje acumulado 2022: 0%

1.4 Proceso Recursos Físicos y Suministros

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de activos de información por ausencia de controles de acceso físico	Actualizar la documentación de las zonas seguras de la Entidad definiendo los controles de acceso físico requeridos, así como las medidas de protección contra desastres naturales, ataques maliciosos o accidentes.	No se reportaron avances por parte del proceso. **Porcentaje trimestre:** 0%

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
	Designar a un responsable para el monitoreo permanente del Circuito Cerrado de Televisión de la Entidad. Realizar monitoreo en tiempo real del CCTV.	No se reportaron avances por parte del proceso. **Porcentaje trimestre:** 0%

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ Se recomienda iniciar la gestión por parte del Grupo Administrativo, para llevar a cabo la actualización de zonas seguras de la Entidad, con el fin de establecer los controles requeridos por parte de cada una de las dependencias responsables de estas áreas para mantener seguros los activos almacenados en las mismas. Es importante que estos controles incluyan medidas de protección contra desastres naturales, ataques maliciosos o accidentes. Así mismo es importante que el personal designado para el monitoreo del CCTV puede llevar a cabo una gestión permanente con el fin de evidenciar posibles eventos de seguridad de información. Lo anterior con el fin de aportar de esta manera en la ejecución de controles previamente establecidos y la mitigación de los riesgos de seguridad de información del proceso.
- ✓ Porcentaje de avance del 3 trimestre: 0%.
- ✓ Porcentaje acumulado 2022: 0%.

1.5 Proceso gestión de talento humano

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de confidencialidad de las historias laborales de los funcionarios.	Unificar matrices digitales de control de documentos que deben reposar en historia laboral	No se reportaron avances por parte del proceso. **Porcentaje trimestre:** 0%

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ Se recomienda incluir en la matriz de control los documentos digitales entregados por los funcionarios, con el fin de contar con la trazabilidad de documentación que conforma las hojas de vida de los funcionarios y de esta manera ejecutar el control y la actividad establecida como tratamiento de riesgo.
- ✓ Porcentaje de avance del 3 trimestre: 0%.
- ✓ Porcentaje acumulado 2022: 80%

1.6 Proceso gestión jurídica

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de confidencialidad de información clasificada y reservada	Actualizar el A2-FO-03 Índice de Información Clasificada y Reservada con la información suministrada por las dependencias, realizar su correspondiente aprobación y publicación en el portal web de la Entidad.	La Oficina Asesora Jurídica, la Oficina de Tecnología y el Grupo de Gestión Documental, han culminado el proceso de levantamiento de los activos de información de los 14 procesos activos con la respectiva aprobación por parte de cada uno de los líderes de proceso. Con los activos de información como insumo principal se inicia la elaboración del Índice de Información Clasificada y Reservada. **Porcentaje trimestre:** 5%

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ De acuerdo a las evidencias aportadas se observa la actualización de los inventarios de activos de información por proceso. Se recomienda avanzar con la validación jurídica de los activos de información con el fin de establecer la normatividad vigente aplicable para mantener la reserva de aquellos activos catalogados como clasificados o reservados. Adicionalmente teniendo en cuenta que existe la posibilidad que se presenten solicitudes de consulta de información reservada por parte de los ciudadanos o los interesados en general, mientras no se cuente con el índice de información clasificada y reservada formalizado, se recomienda a la Oficina Jurídica apoyar a las dependencias en la generación de conceptos jurídicos requeridos para denegar el acceso a esta información conforme lo establece la ley.
- ✓ Porcentaje de avance del 3 trimestre: 5%.

✓ Porcentaje acumulado 2022: 55%

1.7 Proceso gestión de establecimientos de reclusión

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de disponibilidad y confidencialidad de información de la SUBAER	Realizar seguimiento al cumplimiento y asistencia a las actividades de sensibilización	La Oficina de Tecnología compartió invitación para participar en la charla de sensibilización de seguridad de información y se contó con la participación de algunos funcionarios de la SUBAER **Porcentaje trimestre:** 30%
	Definir método de operación y formato para el reporte del estado de los equipos asignados a los funcionarios de la SUBAER	Los funcionarios enlace asimilaron totalmente la ruta para la presentación de requerimientos frente a las novedades que presentaban los equipos u otras novedades del área de tecnología. **Porcentaje trimestre:** 0% **Nota OTEC**: Esta actividad se culminó en el segundo trimestre.
	Solicitar el requerimiento para la actualización, mantenimiento o reparación de los equipos portátiles o clientes livianos asignados a los funcionarios de la SUBAER	Se hizo entrega de 33 equipos de cómputo a los funcionarios enlace que manifestaron presentar fallas en sus equipos. Se efectuó la devolución de los que presentaban fallas toda vez que fueron asignados hace más de 8 años y no cumplían con los requerimientos básicos o por uso presentaban fallas. **Porcentaje trimestre:** 40%

Observaciones Segunda línea de defensa (Oficina de Tecnología):

✓ Aunque se cuenta con el cambio de 33 equipos portátiles asignados al personal de la SUBAER, se continúa sin evidenciar el reporte por parte de sus funcionarios frente al estado de los equipos portátiles institucionales o clientes livianos, de acuerdo a lo establecido en el control de la matriz de riesgos de seguridad. Es importante que los funcionarios notifiquen a la mesa de ayuda los inconvenientes

detectados con los equipos que tienen a cargo según lo establecido en el procedimiento Gestión de solicitudes de soporte técnico.

- ✓ Porcentaje de avance del 3 trimestre: 23%.
- ✓ Porcentaje acumulado 2022: 63%

1.8 Proceso gestión de tecnologías de la información

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
Pérdida de disponibilidad y confidencialidad de información alojada en activos tipo software o servicios (internos y/o externos)	Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento Gestión de Acceso a Usuarios.	Con el fin de lograr un registro oportuno referente a la habilitación y deshabilitación de cuentas de usuarios, se procedió a actualizar el procedimiento de gestión de usuarios y se remitió a la OAPLA para su revisión y dentro del alcance de este documento se creó el formato de paz y salvo con el fin de lograr una mayor trazabilidad de los usuarios que se retiran de la Entidad. Adicionalmente se delegó a un funcionario de la OTEC para llevar a cabo el registro de usuarios nuevos y deshabilitados a través del formato A3-FO-49 Trazabilidad de Cuentas de Usuario. **Porcentaje trimestre:** 20%
Indisponibilidad de la plataforma tecnológica	Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento de control de cambios.	Durante el semestre se realizaron los siguientes cambios: * Despliegue escritorios virtuales con la nueva plantilla * Cambio de reglas de navegación y configuración del Firewall * Habilitación del ambiente gráfico para los escritorios de Infraestructura y Prensa. * Actualización de la plataforma de portal web * Actualización de intranet **Porcentaje trimestre:** 50%

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
	Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento de gestión de la capacidad	Durante el trimestre no se llevó a cabo el diligenciamiento de registros establecidos en el procedimiento de gestión de la capacidad, es decir que no se cumplió con la actividad del control. Lo anterior teniendo en cuenta el volumen de trabajo del personal a cargo de esta gestión. **Porcentaje trimestre:** 0%
	Ejecutar el plan de remediación de vulnerabilidades de la plataforma tecnológica.	Teniendo en cuenta las actividades de remediación definidas, se realizó el parcheo para remediar la vulnerabilidad de Pure Storage y se habilitaron unas opciones de seguridad. Se actualizó al último firmware disponible y se solicitó al fabricante una ampliación del almacenamiento. Pese a la gestión realizada durante el trimestre, no se llevó a cabo el análisis del plan de remediación de vulnerabilidades con el fin de determinar la cantidad de vulnerabilidades mitigadas. **Porcentaje trimestre:** 0%

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ Se recomienda continuar con la formalización del documento gestión de acceso a usuarios con el fin de dar a conocer a todos los usuarios involucrados las actividades requeridas para lograr el alcance del procedimiento y continuar con la implementación del control establecido.
- ✓ Se evidencia la implementación del control establecido de acuerdo a las evidencias de las actualizaciones realizadas durante el trimestre y tomando como referencia lo establecido en el procedimiento de control de cambios.
- ✓ Con el fin de mitigar el riesgo de indisponibilidad de la plataforma tecnológica, es importante ejecutar los controles establecidos, analizando la información generada en el monitoreo de los servicios y activos de TI versus los umbrales establecidos por la dependencia.
- ✓ Aunque se cuenta con avance en la gestión de las actividades de remediación de vulnerabilidades es importante evaluar esta labor frente al plan de remediación definido con el fin de determinar las acciones pendientes en pro del afinamiento de la plataforma tecnológica.

- ✓ Porcentaje de avance del 3 trimestre: 17.5%.
- ✓ Porcentaje acumulado 2022: 62.5%

2. CONCLUSIONES Y RECOMENDACIONES

Teniendo en cuenta los lineamientos establecidos en la Política de seguridad, privacidad de información y seguridad digital (Resolución 000181 de 2022), es importante que los líderes de proceso, realicen seguimientos al interior de su dependencia con el fin de identificar las actividades establecidas para mitigar riesgos de seguridad de información, así como el cumplimiento de las acciones propuestas.

De un total de 11 riesgos de seguridad digital identificados por los diferentes procesos institucionales se generaron acciones para mitigar 5 de ellos. En conclusión, los procesos institucionales avanzaron con respecto a los indicadores propuestos de la siguiente forma:

PROCESO	PORCENTAJE DE AVANCE III TRIMESTRE	PORCENTAJE ACUMULADO 2022
Gestión de Contractual	0%	0%
Gestión Infraestructura	7%	30%
Gestión de bienes y prestación de servicios	0%	0%
Gestión de recursos físicos y suministros	0%	0%
Gestión Talento Humano	0%	80%
Gestión Jurídica	5%	55%
Gestión de Atención a Establecimientos de Reclusión	23%	63%
Gestión de Tecnologías de la Información	18%	63%

De acuerdo a las actividades ejecutadas y reportadas por los procesos institucionales, durante el tercer trimestre se avanzó en un 7% y un porcentaje acumulado para el año de 30%.

Aprobó: Imelda Muñoz Mancipe
Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal
Profesional Especializado