Informe de gestión trimestral

Plan de Tratamiento de Riesgos de Seguridad en la información

Segundo Trimestre de 2022
Presentado Julio 15 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.	Control 1: Por medio de la actualización del Formulario A3-FO-49 (trazabilidad de cuentas) de las cuentas solicitadas a Colombia compra eficiente para tienda tienda virtual, y los accesos aprobados para SECOP II. Continuamos con el seguimiento y control de los usuarios creados, dando control al riesgo. Control 2. Las compras realizadas por tienda virtual están en cabeza de las áreas misionales. Actividad de control: a la fecha no tenemos avance en la actualización del procedimiento. **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 2 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 realizó la actualización de la circular que contiene los lineamientos para el uso de portátiles en la Entidad, este documento se remitió para revisión al Grupo Administrativo, con corte al 30 de junio no

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
		se contaba con la retroalimentación. Una vez se cuente con el documento formalizado se procederá con su divulgación al personal de la Entidad para su aplicación. **Porcentaje trimestre: 10%**
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: 30%**
Pérdida de confidencialidad de los planos de los ERONES	Actualizar la directriz para el manejo de planos institucionales incluyendo lineamientos para el	El control de la entrega de planos físicos para consulta de acuerdo Directriz préstamo y/o consulta de planos de la DINFRA, debe

RIESGO	ACTIVIDAD	AVANCE (Información reportada por el proceso)
	acceso de personal externo de la Entidad, y documentar en un método de operación.	ser consignado en el formato IN-FO-019 . El soporte de los formatos diligenciados y aprobados se encuentran en la carpeta compartida de la DINFRA. Se anexa soporte formato actualizado préstamo y/o 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: 30%**

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.
- ✓ Se evidencia la definición y aplicación de lineamientos para la verificación del cargue de información gestionada por parte del personal de la DINFRA, se recomienda avanzar en su formalización a través de un método de operación de acuerdo a la actividad definida como tratamiento de riesgo.
- ✓ Se evidencia la definición y aplicación del control para el manejo de planos institucionales, se recomienda avanzar en su formalización a través de un método de operación de acuerdo a la actividad definida como tratamiento de riesgo.
- ✓ Porcentaje de avance del 2 trimestre: 23%.
- ✓ Porcentaje acumulado 2022: 23%

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.	Se instruyó la formulación del procedimiento para el manejo y seguridad de la información reportada en el listado censal de la población privada de la libertad, el cual está en elaboración. Se estima que, durante el tercer trimestre de la vigencia 2022 se entregue aprobado dicho documento por parte de la Subdirección de Servicios a través de la Oficina Asesora de Planeación. **Porcentaje trimestre: 0%**
	Realizar seguimiento al cumplimiento del lineamiento establecido.	Esta actividad depende de la anterior. **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 2 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%
	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 2 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	Teniendo en cuenta el periodo de la pandemia los servidores públicos dirigieron sus comunicaciones vía correo electrónico los cuales hacen parte del archivo virtual del Grupo Administración de Personal, sin embargo se habilitará una pestaña a la matriz de control relacionada con las incapacidades. **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 2 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 conjuntamente con la Oficina de Tecnología y el Grupo de Gestión Documental, con el propósito de verificar la confidencialidad de la información, de acuerdo a la normatividad jurídica vigente y con el fin de evitar el acceso a personas no autorizadas, continua la actualización del Inventario de Activos de Información y del Índice de Información Clasificada y Reservada , revisando para el periodo con los delegados los siguientes procesos: Gestión Contractual, Gestión de la Comunicación Institucional, Gestión de las Tecnologías de la Información, Gestión de Recursos Físicos y Suministros, Gestión de Suministro de Bienes y Prestación de Servicios, Gestión del Talento Humano, Gestión Documental, Gestión Jurídica y Evaluación de la Gestión Institucional. **Porcentaje trimestre:** 20%

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ De acuerdo a las evidencias aportadas se observa la implementación de la actividad de tratamiento establecida para la presente vigencia. Se recomienda continuar avanzando en la gestión de actualización del índice de información clasificada y reservada con el fin de llevar a cabo la verificación de la confidencialidad de la información, de acuerdo a la normatividad jurídica vigente en caso requerido por alguna dependencia de la Entidad y evitar así el acceso a personas no autorizadas.
- ✓ Porcentaje de avance del 2 trimestre: 20%.
- ✓ Porcentaje acumulado 2022: 50%

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	Para este periodo no fueron programadas capacitaciones para la Subdirección Atención a los Establecimientos de Reclusión. **Porcentaje trimestre:** 0%
	Definir método de operación y formato para el reporte del estado de los equipos asignados a los funcionarios de la SUBAER	Las solicitudes se vienen tramitando mediante el correo mesadeayuda@uspec.gov.co, según lo establecido en el procedimiento Gestión de solicitudes de soporte técnico definido por la Oficina de Tecnología. **Porcentaje trimestre:** 40%
	Solicitar el requerimiento para la actualización, mantenimiento o reparación de los equipos portátiles o clientes livianos asignados a los funcionarios de la SUBAER	Teniendo en cuenta lo actuado en el primer trimestre se adquirieron y asignaron equipos de cómputo para la SUBAER mediante orden de compra 83844, se realizó un análisis y filtro de quienes requieren equipo con mayor prioridad de acuerdo al estado de los mismos, aclarando que el cambio de equipos se hace necesario a todos los funcionarios, el día 23 de mayo 2022, se remitió el listado de seriales por parte de la OTEC al área administrativa teniendo en cuenta que estos equipos serán asignados al personal que labora en los establecimientos deben tener una configuración adicional. La entrega se hará en el mes de julio. Para la entrega de los equipos se dio prioridad de cambio a los equipos en mal estado que presentaban daños graves a moderados . **Porcentaje trimestre:** 0%

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ Teniendo en cuenta que todas las solicitudes de soporte técnico se canalizan a través de un único medio establecido por la Oficina de Tecnología como responsable de la mesa de ayuda y establecido a través del procedimiento Gestión de solicitudes de soporte técnico, se toma como ejecutada la acción propuesta en cuanto a la definición del método de operación. Se recomienda a la SUBAER realizar seguimiento al personal adscrito a su dependencia, con el fin de que todas las solicitudes del estado de los equipos que tienen asignados se reporten de manera oportuna a través del canal establecido.

- ✓ Se evidencia la gestión para el cambio de los portátiles del personal de la SUBAER, sin embargo no se evidencia el análisis de criterios que conllevo a la asignación de los mismos. Con el fin de avanzar con la implementación del control descrito "Establecer reporte por parte de los funcionarios de la SUBAER frente al estado de los equipos portátiles institucionales o clientes livianos" es importante que los funcionarios notifiquen a la mesa de ayuda los inconvenientes detectados con los equipos que tienen a cargo.

- ✓ Porcentaje de avance del 2 trimestre:13%.

- ✓ Porcentaje acumulado 2022: 40%

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.	Durante el segundo semestre se realizó seguimiento a los registros del procedimiento de gestión de usuarios, identificando cambios adicionales a los definidos en el primer trimestre del año. En cuanto al control establecido, no se está registrando oportunamente la información referente a la habilitación y deshabilitación de cuentas de usuario en el formato A3-FO-49 Trazabilidad de Cuentas de Usuario, por lo tanto desde la OTEC se plantea delegar esta gestión en un único funcionario, una vez si finalice la gestión requerida. **Porcentaje trimestre:** 10%

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: * Cambio de plataforma de correo colaborativa Zoho a Google Workspace versión Enterprise Standard. Aunque no se documentó en el formato establecido, se tomaron las medidas necesarias para la mitigación de los riesgos del cambio. * Herramienta de inventarios * Reconfiguración de las redes inalámbricas. * Instalación del agente de Rapid7 en la instancia de cómputo de Google Cloud Platform. * Remediación de conjunto de vulnerabilidades asociadas a protocolo SSL y suite de cifrado en servidores Windows. **Porcentaje trimestre:** 50%
	Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento de gestión de la capacidad	Se realizó el respectivo seguimiento, sin embargo durante el semestre 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 volúmen de trabajo del personal a cargo de esta gestión. **Porcentaje trimestre:** 0%
	Ejecutar el plan de remediación de vulnerabilidades de la plataforma tecnológica.	Durante el segundo trimestre se llevó a cabo un nuevo análisis de vulnerabilidades, ejecutado a 655 activos (entre estos 96 servidores, equipos de red y seguridad, los restante corresponden a sistema de clientes), del cual resultaron 1155 vulnerabilidades de nivel altas y críticas (los 2 niveles mas altos que usa la herramienta utilizada por el contratista) para un total de 4055 vulnerabilidades; (incluidas las 1028 vulnerabilidades provenientes del primer trimestre) en el segundo trimestre del 2022 se realizó la remediación efectiva de 693 vulnerabilidades, comprobadas a través de análisis de re-test, en contraste a las actividades de remediación ejecutadas, 20 vulnerabilidades a las que

		se realizó gestión persisten. En conclusión de un total de 1172 vulnerabilidades catalogadas como altas y críticas, durante el primer semestre se han resulto 837. **Porcentaje trimestre:** 58%

Observaciones Segunda línea de defensa (Oficina de Tecnología):

- ✓ Es importante que se asegure la trazabilidad de la habilitación y deshabilitación de cuentas de usuarios con el fin de mitigar el riesgo y que se conserve información documentada como evidencia de la ejecución del procedimiento. Adicionalmente se considera necesario formalizar a través de la actualización del procedimiento los cambios evidenciados en las revisiones.
- ✓ Se evidencia la implementación del control de cambios de acuerdo a las evidencias de las actualizaciones realizadas durante el semestre, sin embargo es importante documentar todos los cambios de acuerdo a los formatos establecidos por la dependencia a través del 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.
- ✓ Se evidencia la ejecución del plan de remediación definido para remediar las vulnerabilidades de la plataforma tecnológica, cumpliendo de esta forma con la implementación del control propuesto.
- ✓ Porcentaje de avance del 2 trimestre: 29%.
- ✓ Porcentaje acumulado 2022: 45%

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 II TRIMESTRE	PORCENTAJE ACUMULADO 2022
Gestión de Contractual	0%	0%

Gestión Infraestructura	23%	23%
Gestión de bienes y prestación de servicios	0%	0%
Gestión de recursos físicos y suministros	0%	0%
Gestión Talento Humano	0%	80%
Gestión Jurídica	20%	50%
Gestión de Atención a Establecimientos de Reclusión	13%	40%
Gestión de Tecnologías de la Información	29%	45%

De acuerdo a las actividades ejecutadas y reportadas por los procesos institucionales, durante el segundo trimestre se avanzó en un 11% y un porcentaje acumulado para el año de 30%.

Aprobó: Imelda Muñoz Mancipe
Jefe Oficina de Tecnología

Revisó: Camilo Alejandro Romero González
Coordinador Grupo Comunicaciones

Elaboró: Mayra Alexandra Agudelo Carvajal
Profesional Especializado