PRIMER INFORME DE LOS TRATAMIENTOS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Grupo de Trabajo de Informática Forense y Seguridad Digital
Oficina de Tecnología e Informática
Superintendencia de Industria y Comerio

Junio 2025

Superintendencia de Industria y Comercio

Contenido

1. GLOSARIO

ACTIVIDAD (Plan de tratamiento del riesgo): acciones tendientes a fortalecer los controles identificados para mitigar los riesgos o a prevenir las causas señaladas en la identificación del riesgo.

PLAN DE TRATAMIENTO DEL RIESGO: actividades tendientes a mejorar los controles identificados para mitigar los riesgos o las causas que originan el riesgo, los responsables de ejecutar dichas actividades y las fechas de ejecución.

RIESGO: posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

2. INTRODUCCIÓN

La Oficina Asesora de Planeación solicitó en marzo de 2025 a los líderes de cada proceso, la actualización o identificación de nuevos riesgos, que para el caso del riesgo de seguridad de la información es aquello que puede afectar la confidencialidad, disponibilidad e integridad de la información institucional. La identificación del riesgo incluye actualizar los controles y su valoración frente a la probabilidad e impacto, y el planteamiento de las actividades a desarrollar en la vigencia 2025, las cuales están orientadas a tratar las causas del riesgo, al fortalecimiento de los controles identificados o a la identificación de nuevos mecanismos para prevenir la materialización del riesgo.

La OTI a través del Grupo de trabajo de Informática Forense y Seguridad Digital brinda el acompañamiento a las áreas que lo requieran en la revisión adecuada de los riesgos y los controles para la mitigación de los mismos que han establecido los líderes de los procesos, y recomienda los debidos ajustes a que haya lugar.

El presente informe contiene el avance del seguimiento a los tratamientos de riesgos de seguridad de la información correspondientes al primer y segundo trimestre del 2025.

3. ACTUALIZACIÓN A LOS TRATAMIENTOS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

De los 45 procesos que conforman la estructura organizacional de la entidad, 44 identificaron riesgos en la categoría de seguridad de la información, siendo en total 50 riesgos distribuidos de la siguiente manera: 17 riesgos de integridad, 10 riesgos de confidencialidad, 20 riesgos de disponibilidad, 1 riesgo combinado de integridad y disponibilidad, 1 riesgo combinado de confidencialidad y disponibilidad, y 1 riesgo combinado de integridad, confidencialidad y disponibilidad.

El proceso Gestión Integral de Datos Personales previamente ha identificado sus activos de información para próximamente definir el riesgo de seguridad de la información.

En total son 97 actividades a las cuales dar cumplimiento, distribuidas de la siguiente manera: 3 para el primer trimestre, 13 para el segundo trimestre, 11 para el tercer trimestre y 70 para el cuarto trimestre.

3.1 CAMBIOS EJECUTADOS EN LOS TRATAMIENTOS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1) El proceso GF03 TESORERÍA cambió la descripción del riesgo.

Riesgo anterior	Riesgo actual
PÉRDIDA DE DISPONIBILIDAD - al no contar oportunamente con las herramientas tecnológicas y sus bases datos que permitan gestionar la información que soportan las transacciones y operaciones de viáticos.	PÉRDIDA DE DISPONIBILIDAD - al no contar oportunamente con las herramientas tecnológicas y sus bases datos que permitan gestionar la información que soportan las transacciones y operaciones de pagos.

Descripción anterior	Descripción actual
Posibilidad de afectación económica y/o reputacional por falta de disponibilidad de la herramienta tecnológica (SIC COMISIONA) definida en la matriz de activos de la información, así como de la información contenida en las mismas para cumplir con las obligaciones operativas y legales, en materia de gestión de viáticos debido a fallas tecnológicas o casos fortuitos o imprevisibles.	Posibilidad de afectación económica y/o reputacional por falta de disponibilidad de la herramienta tecnológica (DERECHO AL TURNO) definida en la matriz de activos de la información, así como de la información contenida en las mismas para cumplir con las obligaciones operativas y legales, en materia de gestión de viáticos debido a fallas tecnológicas o casos fortuitos o imprevisibles.

2) El proceso GF02 PRESUPUESTAL, cambió la actividad para la actual vigencia:

Riesgo anterior	Riesgo actual
PÉRDIDA DE INTEGRIDAD - Pérdida de integridad de la información financiera relacionada con la serie de certificados, informes de ejecución presupuestal, reportes de contabilidad presupuestal y solicitudes de modificación presupuestal en medio digital.	PÉRDIDA DE INTEGRIDAD de la información financiera relacionada con los Registro Presupuestales en medio digital (Onedrive)

Descripción anterior	Descripción actual
Posibilidad de afectación reputacional por pérdida de credibilidad y confianza de los grupos de valor, partes interesadas y Entes de Control. Debido a la perdida de integridad y disponibilidad de la información presupuestal en medio digital por la falta de controles del espacio de almacenamiento	Posibilidad de afectación reputacional por pérdida de credibilidad y confianza de los grupos de valor, partes interesadas y Entes de Control debido a la perdida de integridad y disponibilidad de los registros presupuestales en medio digital por la falta de controles del espacio de almacenamiento.

3) El proceso GS04 GESTIÓN DE INFORMÁTICA FORENSE cambió el riesgo.

Riesgo anterior	Riesgo actual
PÉRDIDA DE CONFIDENCIALIDAD - Durante el transporte de evidencias digitales.	PÉRDIDA DE CONFIDENCIALIDAD - Y DISPONIBILIDAD durante el transporte de evidencias digitales.

4) El proceso SC05 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN cambió el riesgo.

Riesgo anterior	Riesgo actual
PÉRDIDA DE CONFIDENCIALIDAD - Ante ataques cibernéticos de tipo de ingeniería social, que comprometan la información de la Entidad durante el trabajo remoto.	PÉRDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD de la información de la Entidad ante un incidente de seguridad que comprometa los activos de información.

Descripción anterior	Descripción actual
Posibilidad de afectación reputacional por la materialización de incidentes de seguridad de la información debido a que el trabajo remoto en la SIC implica nuevos vectores de ataque, lo cual puede ocasionar incidentes que afecte la información de la entidad. Activos de información afectados: Activos cuyo medio de conservación y/o soporte es digital y/o electrónico de los procesos de la entidad.	Posibilidad de afectación operacional, financiera, reputacional o legal por la materialización de incidentes de seguridad de la información debido al incumplimiento de los controles de seguridad de la información establecidos por la entidad. Los activos afectados incluyen medios de conservación, soportes electrónicos, sistemas de información y cualquier otro recurso tecnológico que maneje datos críticos para la Entidad.

5) Los procesos PI01 Registro y depósito de signos distintivos, PI02 Concesión de nuevas creaciones y PI03 Transferencia de información tecnológica basada en patentes, eliminaron el siguiente control:

Control	Justificación
Domino: A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. Objetivo: A17.1 Continuidad de seguridad de la información. Control: A.17.1.2 Implementación de la continuidad de la seguridad de la información. El Servidor público del Grupo de Servicios Tecnológicos cuando se requiera, activa el Plan de Recuperación ante desastres - DRP de la aplicación el cual se encuentra en el Data Center Alterno Bochica. Cuando se detecte indisponibilidad de la aplicación en Nébula, la infraestructura de la aplicación alojada en Bochica asume el servicio. Como evidencia del control se cuenta con los logs relacionados en Nutanix. Se encuentra documentado en el BIA y en el manual del DRP. De acuerdo con lo establecido en el SC05-F06, SC05-F11 y en el instructivo SC05-I07.	La infraestructura del Plan de Recuperación ante Desastres (DRP) no se encuentra disponible actualmente, debido a que la plataforma de virtualización en la que fue construida ha dejado de contar con soporte. En este sentido, la Oficina de Tecnologías de la Información (OTI) se encuentra en el proceso de adquisición de una nueva plataforma de virtualización. No obstante, esta transición implica la migración de la infraestructura actual a la nueva plataforma, lo que tomará un tiempo considerable para su implementación. Dado lo anterior, y considerando que la infraestructura del DRP no estará operativa durante la presente vigencia, solicitamos la eliminación del control relacionado con el DRP para este período.

4. SEGUIMIENTO A LAS ACTIVIDADES DEFINIDAS EN LOS TRATAMIENTOS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El seguimiento se ejecutó enviando un correo electrónico a los enlaces de las respectivas áreas, con el fin que confirmaran si las actividades estaban siendo gestionadas o si requerían apoyo por parte de la OTI para darles cumplimiento.

Se recibió respuesta vía correo electrónico por parte de los enlaces de procesos, confirmando la ejecución o no de las actividades dentro de las fechas establecidas. También se confirma su ejecución a través del módulo de monitoreo de riesgos de gestión en la herramienta del SIGI.

- Para el primer trimestre se identificaron las siguientes actividades a las cuales se les debería dar cumplimiento:

PROCESO	RIESGO	ACTIVIDAD	PRODUCTO ESPERADO	FECHA FIN	ESTADO
ASESORÍA Y EVALUACIÓN INDEPENDIENTE	PÉRDIDA DE INTEGRIDAD de los expedientes, contratos, informes y otros que se entregan en custodia a la OCI como parte del ejercicio de auditoría, seguimientos, monitoreos e informes de Ley seguimiento.	Realizar análisis a la necesidad de actualizar la matriz de riesgos de gestión y corrupción del proceso a cargo de la OCI.	Propuesta de ajuste matriz de riesgos.	31/03/2025	Actividad cumplida por el área.
	PÉRDIDAD DE DISPONIBILIDAD de la información asociada a la ejecución del Plan Anual de Auditorías Internas (papeles de trabajo, informe preliminar, informe final, entre otros).	Realizar consulta a la OTI respecto a la posibilidad de disponer de un servidor que sirva como repositorio de los informes generados por la OCI para auditorías, informes de ley y seguimientos.	Memorando consulta a la OTI sobre la posibilidad de disponer de un servidor que sirva como repositorio de los informes generados por la OCI para auditorías, informes de ley y seguimientos.	31/03/2025	Actividad cumplida por el área.

PROCESO	RIESGO	ACTIVIDAD	PRODUCTO ESPERADO	FECHA FIN	ESTADO
REGISTRO Y DEPÓSITO DE SIGNOS DISTINTIVOS	PÉRDIDAD DE DISPONIBILIDAD - con ocasión a caídas del sistema de información de propiedad industrial SIPI debido a fallas presentadas en el sistema o de la infraestructura que lo soporta.	Documentar el control. El servidor público o contratista de la Dirección de Signos Distintivos cada vez que se presente indisponibilidad del SIPI, debe remitir un correo electrónico al Centro de servicios integrados TI con el fin de que la OTI gestiones las acciones pertinentes para la solución de la indisponibilidad. La evidencia de la ejecución del control son los correos electrónicos dirigidos a Centros de servicios Integrados de TI (Mesa de ayuda)	Documento	31/03/2025	Actividad cumplida por el área.

- Para el segundo trimestre se identificaron las siguientes actividades a las cuales se les debería dar cumplimiento:

PROCESO	RIESGO	ACTIVIDAD	PRODUCTO ESPERADO	FECHA FIN	ESTADO
SERVICIOS ADMINISTRATIVOS	PÉRDIDAD DE INTEGRIDAD - de la información institucional ante accesos no autorizados a la Entidad.	Revisar, actualizar y socializar la circular de seguridad y vigilancia para la vigencia 2025.	Circular actualizada	30/04/2025	Actividad cumplida por el área.
TRÁMITES ADMINISTRATIVOS PROTECCIÓN DE DATOS PERSONALES	PÉRDIDA DE CONFIDENCIALIDAD - ante la divulgación no autorizada de información de expedientes.	Socializar con la OTI el requerimiento del informe cuatrimestral con el listado de usuarios con acceso a los sistemas de información de la Delegatura, para explicar su importancia como control para mitigar el riesgo de pérdida de confidencialidad de la información de expedientes.	Listado de asistencia	10/04/2025	Actividad cumplida por el área.
SEGUIMIENTO SISTEMA INTEGRAL DE GESTIÓN INSTITUCIONA_	PÉRDIDA DE INTEGRIDAD - del Sistema Integral de Gestión Institucional	Realizar depuración de los perfiles y usuarios autorizados en el SIGI.	Evidencias del SIGI, archivo excel exportado.	30/05/2025	Actividad cumplida por el área.
FORMULACIÓN SISTEMA INTEGRAL DE GESTIÓN	PÉRDIDA DE INTEGRIDAD - del Sistema Integral de Gestión Institucional	Realizar depuración de los perfiles y usuarios autorizados en el SIGI.	Evidencias del SIGI, archivo excel exportado.	30/05/2025	Actividad cumplida por el área.

NOTIFICACIONES	PÉRDIDA DE CONFIDENCIALIDAD - una indebida notificación a una dirección errónea.	Realizar mesa de trabajo con los enlaces de numeración de todas las delegaturas y la OAP, donde se indiquen las causas de devolución de actos administrativos, para así prevenir errores en la planilla de numeración y evitar retrocesos en el proceso.	Informe de estado de funcionamiento de la planilla electrónica.	30/05/2025	Actividad cumplida por el área.
TRÁMITES ADMINISTRATIVOS PROTECCIÓN DE DATOS PERSONALES	PÉRDIDA DE CONFIDENCIALIDAD - ante la divulgación no autorizada de información de expedientes	Definir el cronograma de capacitación interna que contemple los temas clave en seguridad de la información, estableciendo el periodo y la frecuencia en la que se desarrollarán las sesiones. Esto permitirá fortalecer el conocimiento de los servidores públicos y contratistas sobre las medidas de protección de datos y minimizar el riesgo de divulgación no autorizada.	Cronograma de capacitación interna	16/05/2025	Actividad cumplida por el área.

SERVICIOS ADMINISTRATIVOS	PÉRDIDAD DE INTEGRIDAD - de la información institucional ante accesos no autorizados a la Entidad.	Realizar socialización al personal de vigilancia sobre establecido en la circular de seguridad y vigilancia para la vigencia 2025.	Socialización realizada.	30/05/2025	Actividad cumplida por el área.
TESORERÍA	PÉRDIDA DE DISPONIBILIDAD - al no contar oportunamente con las herramientas tecnológicas y sus bases datos que permitan gestionar la información que soportan las transacciones y operaciones de pagos.	Realizar capacitación a los colaboradores del proceso de tesorería en relación al procedimiento para reportar fallas en los aplicativos	Presentación de capacitación	30/06/2025	Actividad cumplida por el área.
INVENTARIOS	PÉRDIDA DE INTEGRIDAD - durante la gestión de la información de los inventarios en Helisa.	Gestionar la capacitación al equipo de trabajo del grupo de SAyRF en las políticas seguridad de la información implementadas por la entidad.	capacitación realizada	30/06/2025	Actividad cumplida por el área.
		Socializar la actualización de la matriz de activos de la información a los funcionarios y Contratistas del grupo de SAyRF,	capacitación realizada	30/06/2025	Actividad cumplida por el área.
SEGURIDAD Y SALUD EN EL TRABAJO	PÉRDIDA DE CONFIDENCIALIDAD - ante inadecuado manejo de las bases de datos de diagnósticos médicos	Definir las personas responsables que deben tener acceso a la plataforma de Hession.	Correo electrónico por parte del Coordinador del Grupo Asignado esa responsabilidad.	30/06/2025	Actividad cumplida por el área.

PROTECCION DE USUARIOS DE SERVICIOS DE COMUNICACIONES	PÉRDIDA DE INTEGRIDAD - Por modificación de la Información allegada a través de aplicaciones que permiten almacenamiento y envio de informacion (we transfer, links de descarga, etc) por parte de los operadores de servicios de comunicaciones.	Creación de formulario. Con el objetivo de realizar acciones que permitan continuar con la mitigación del riesgo perdida de la integridad y lograr obtener una información veraz y consistente en los datos ingresados al sistema de protección yo sistema de trámites, se creará un formulario para el levantamiento de información que permita evidenciar las probables causas o errores más comunes al momento de evaluar, transcribir o radicar los documentos (denuncias) ingresados a la Dirección.	Entrega del link de acceso yo pantallazos del formulario	30/06/2025	Actividad cumplida por el área.
GESTIÓN DE INGRESOS Y DEVOLUCIONES	PÉRDIDA DE DISPONIBILIDAD - al no contar oportunamente con la herramienta tecnológica y sus bases datos que permita gestionar la información de ingresos y TDJ dentro del término legal.	Realizar capacitación a los colaboradores del proceso de ingresos en relación al procedimiento para reportar fallas en los aplicativos	Presentación de capacitación	30/06/2025	Actividad cumplida por el área.

5. CONCLUSIÓN

En conclusión, se evidencia que cada una de las áreas gestionaron las actividades planeadas a ejecutarse en el primer y segundo trimestre: en marzo 3 actividades, en abril 2 actividades, en mayo 5 actividades y en junio 6 actividades.
De conformidad con lo anteriormente descrito, se confirma la ejecución de 16 actividades.

Teniendo en cuenta que hasta el momento son en total 97 actividades descritas en los planes de tratamiento de riesgos de seguridad de la información, el avance es del 16,5%.

Elaboró: María Carolina Castro Becerra
Revisó: Magda Julieth Zarrate Saldaña
Aprobó: Magda Julieth Zarrate Saldaña