SEGUNDO 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

Septiembre 2025

Superintendencia de Industria y Comercio

Contenido

1. GLOSARIO 2
2. INTRODUCCIÓN 2
3.1 CAMBIOS EJECUTADOS EN LOS TRATAMIENTOS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 3
4. SEGUIMIENTO A LAS ACTIVIDADES DEFINIDAS EN LOS TRATAMIENTOS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 26
5. CONCLUSIÓN 29

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 para el tercer trimestre del 2025.

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

El proceso CS0CS05 Gestión Integral de Datos Personales identificó dos (2) riesgos de seguridad de la información que afectan la integridad para la actual vigencia, con los cuales, se estableció una actividad para cada riesgo.

El proceso CI01 Asesoría y Evaluación Independiente eliminó dos riesgos, uno de integridad y el otro de disponibilidad, y creó un riesgo de confidencialidad.

Por lo tanto, se identifican 3 riesgos nuevos de seguridad de la información para la actual vigencia.

En los 45 procesos que conforman la estructura organizacional de la entidad se identificaron 51 riesgos en la categoría de seguridad de la información, distribuidos de la siguiente manera: 18 riesgos de integridad, 11 riesgos de confidencialidad, 19 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.

Los procesos de GJ01 Cobro coactivo y SC03 Gestión ambiental identificaron riesgos de seguridad de la información, sin embargo, al valorar el impacto y probabilidad del riesgo y de acuerdo a la metodología para la administración del riesgo, estos fueron ubicados en una zona baja antes de controles, por lo tanto, asumen el riesgo y no es necesario que definieran actividades.

En total son 101 actividades que mitigan los riesgos y a las cuales dar cumplimiento, distribuidas de la siguiente manera: 1 para el primer trimestre, 13 para el segundo trimestre, 11 para el tercer trimestre y 76 para el cuarto trimestre.

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

1) El proceso CS02 FORMACIÓN en junio 2025 cambió la descripción de los controles del riesgo PÉRDIDAD DE DISPONIBILIDAD del campus virtual de la Entidad.

Control anterior	Control actual
Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.3 Reporte de debilidades de seguridad de la información. El servidor público o contratista del Grupo de Formación, realizará el monitoreo mensual al campus virtual externo de la entidad, a través de actividades de verificación y validación de funciones a nivel de aplicación. Cuando se detecte una falla en el campus virtual externo de la entidad, se debe reportar a través de correo electrónico a la Mesa de Servicios de la Entidad, con las evidencias del incidente para su gestión y solución, generando las alertas en las herramientas tecnológicas y, en caso de ser necesario, reasignando los recursos de infraestructura para la continuidad. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales. Se evidencia en un reporte trimestral donde se explique y muestre el correo enviado por el responsable del Grupo de Trabajo de Formación al correo de la mesa de servicios de la entidad. Si no se materializa, se debe entregar el reporte de revisión del historial de disponibilidad del sistema campus virtual, explicando que todo fluyó normalmente, por lo tanto no fue necesario generar las alertas respectivas ni la reasignación de recursos, mostrando las capturas de pantalla correspondientes.	Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.3 Reporte de debilidades de seguridad de la información. El servidor público o contratista del Grupo de Formación, realizará el monitoreo mensual al campus virtual externo de la entidad, a través de actividades de verificación y validación de funciones a nivel de aplicación. Cuando se detecte una falla en el campus virtual externo de la entidad, se debe reportar a través de correo electrónico a la Mesa de Servicios o caso creado directamente en la herramienta de help desk de la entidad, con el aval de la Coordinación del Grupo de Trabajo de Sistemas de Información con las evidencias del incidente para su gestión y solución, generando las alertas en las herramientas tecnológicas y, en caso de ser necesario, reasignando los recursos de infraestructura para la continuidad. Se evidencia en un reporte trimestral donde se explique y muestre el correo enviado a la mesa de servicios o el caso registrado en la herramienta de help desk de la entidad por el responsable del Grupo de Trabajo de Formación. Si no se materializa, se debe entregar el reporte de revisión del historial de disponibilidad del sistema campus virtual, explicando que todo fluyó normalmente, por lo tanto no fue necesario generar las alertas respectivas ni la reasignación de recursos, mostrando las capturas de pantalla correspondientes. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales.

Dos controles correctivos se unificaron en un solo control:

Control anterior	Control actual
Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.2 Reporte de eventos de seguridad de la información. El servidor público o contratista del Grupo de Formación cada vez que se presente pérdida de disponibilidad del campus virtual, enviará correo electrónico a los inscritos en los cursos virtuales, comunicando las nuevas fechas de inscripción y finalización de los cursos. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales. Se evidencia en un reporte trimestral que contenga capturas de pantalla del correo electrónico enviado a los inscritos en los cursos virtuales. Si no se materializa el riesgo, se debe enviar la misma evidencia mostrando el perfecto funcionamiento del campus e informando que no fue necesario enviar correos a los inscritos.	Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.2 Reporte de eventos de seguridad de la información. El servidor público o contratista del Grupo de Formación cada vez que se le notifique o detecte una pérdida de disponibilidad del campus virtual de la entidad, deberá ejecutar una o las dos acciones siguientes: i) publicar en la sede electrónica de la entidad y del campus virtual, una pieza gráfica que informe a la ciudadanía que el campus virtual no se encuentra disponible, sea por falla técnica temporal o por mantenimiento y soporte y / o ii) enviar correo a los estudiantes matriculados en ese momento, informándoles tanto sobre la indisponibilidad del campus, como sobre el restablecimiento del servicio. La elección de la(s) acción(es) a ejecutar dependerá del nivel de impacto y duración estimada del incidente, de acuerdo con los siguientes criterios: • Solo acción i) (pieza gráfica): Aplica cuando la indisponibilidad sea visible públicamente (por ejemplo, caída total del campus virtual) y no interfiere con fechas críticas para la inscripción o finalización de los cursos virtuales. • Solo acción ii) (correo a estudiantes): Aplica cuando la afectación sea temporal (menor a 1 hora)

Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.2 Reporte de eventos de seguridad de la información. El servidor público o contratista del Grupo de Formación cada vez que se presente perdida de disponibilidad del campus virtual de la entidad, enviará correo electrónico al Grupo de Comunicaciones solicitando la elaboración de una pieza gráfica para la ciudadanía, donde se informe que el campus virtual se encuentra en mantenimiento y soporte. Esta pieza deberá publicarse en la sede electrónica de la entidad y del campus virtual. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales. El control se evidenciará trimestralmente mediante la consolidación de un reporte corto donde se registre el monitoreo permanente del comportamiento del campus virtual y la captura de pantalla de la publicación de la pieza gráfica en las páginas web de la SIC y del Campus virtual. En caso de no materializarse el riesgo, se debe evidenciar en un reporte corto que muestre el perfecto funcionamiento del campus durante el periodo.	y exclusiva para estudiantes matriculados, sin necesidad de informar al público general. • Ambas acciones: Se aplican de manera obligatoria cuando la interrupción sea superior a 1 hora, afecte el desarrollo normal de cursos o impacte fechas de inscripción o finalización de cursos. Se evidencia mediante la consolidación de un reporte donde se registre el monitoreo permanente del comportamiento del campus virtual y la captura de pantalla de la publicación de la pieza gráfica en las páginas web de la SIC y del Campus virtual y captura de pantalla aleatoria de algunos correos enviados a los estudiantes, según sea el caso. En caso de no materializarse el riesgo, se debe evidenciar en un reporte que muestre el correcto funcionamiento del campus durante el periodo. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales.

Se actualizó la actividad:

Actividad	Producto esperado
Ampliar las fechas de inscripción y finalización de los cursos en caso de fallas superiores a 48 horas, sobre la infraestructura o plataforma en la cual opera el Campus virtual, informando a los inscritos en los cursos virtuales a través	Un Informe trimestral consolidado del comportamiento de la plataforma Moodle del campus virtual donde se especifiquen las fallas de la plataforma y los cambios en la ampliación de las fechas de inscripción y finalización de los cursos,

de correo electrónico la ampliación de las fechas.	junto con la captura de pantalla aleatoria de algunos correos electrónicos enviados a los inscritos, esto último en caso de ser necesario. Si no se presentan fallas, se debe enviar la misma evidencia mostrando el correcto funcionamiento del campus e informando que no fue necesario enviar correos a los inscritos

2) El proceso CS02 FORMACIÓN en agosto de 2025 cambió la descripción de los controles del riesgo PÉRDIDAD DE DISPONIBILIDAD del campus virtual de la Entidad.

Dos controles correctivos se unificaron en un solo control:

Controles anteriores	**Control actual**

Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.3 Reporte de debilidades de seguridad de la información. El servidor público o contratista del Grupo de Formación, realizará el monitoreo mensual al campus virtual externo de la entidad, a través de actividades de verificación y validación de funciones a nivel de aplicación. Cuando se detecte una falla en el campus virtual externo de la entidad, se debe reportar a través de correo electrónico a la Mesa de Servicios o caso creado directamente en la herramienta de help desk de la entidad, con el aval de la Coordinación del Grupo de Trabajo de Sistemas de Información con las evidencias del incidente para su gestión y solución, generando las alertas en las herramientas tecnológicas y , en caso de ser necesario, reasignando los recursos de infraestructura para la continuidad. Se evidencia en un reporte trimestral donde se explique y muestre el correo enviado a la mesa de servicios o el caso registrado en la herramienta de help desk de la entidad por el responsable del Grupo de Trabajo de Formación. Si no se materializa, se debe entregar el reporte de revisión del historial de disponibilidad del sistema campus virtual, explicando que todo fluyó normalmente, por lo tanto no fue necesario generar las alertas respectivas ni la reasignación de recursos, mostrando las capturas de pantalla correspondientes. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales.	Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.2 Reporte de eventos de seguridad de la información. El servidor público o contratista del Grupo de Formación, realizará el monitoreo mensual el monitoreo de la disponibilidad del campus virtual externo de la entidad, mediante la coordinación con la OTI para la verificación técnica del funcionamiento del sistema y la validación directa de funciones a nivel de aplicación. Cuando se detecte o notifique una pérdida de disponibilidad del campus virtual, se activará el protocolo de gestión de continuidad que incluye: (i)reporte inmediato del incidente a la Mesa de Servicios de la Entidad con las evidencias correspondientes (ii) publicar en la sede electrónica de la entidad y del campus virtual, una pieza gráfica que informe a la ciudadanía que el campus virtual no se encuentra disponible, sea por falla técnica temporal o por mantenimiento y soporte y / o iii) enviar correo a los estudiantes matriculados en ese momento, informándoles tanto sobre la indisponibilidad del campus, como sobre el restablecimiento del servicio. La elección de la(s) acción(es) a ejecutar dependerá del nivel de impacto y duración estimada del incidente, de acuerdo con los siguientes criterios: • Solo acción ii) (pieza gráfica): Aplica cuando la indisponibilidad sea visible públicamente (por ejemplo, caída total del campus virtual) y no interfiere con fechas críticas para la inscripción o finalización de los cursos virtuales. • Solo acción iii) (correo a estudiantes): Aplica cuando la

Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.2 Reporte de eventos de seguridad de la información. El servidor público o contratista del Grupo de Formación cada vez que se le notifique o detecte una pérdida de disponibilidad del campus virtual de la entidad, deberá ejecutar una o las dos acciones siguientes: i) publicar en la sede electrónica de la entidad y del campus virtual, una pieza gráfica que informe a la ciudadanía que el campus virtual no se encuentra disponible, sea por falla técnica temporal o por mantenimiento y soporte y / o ii) enviar correo a los estudiantes matriculados en ese momento, informándoles tanto sobre la indisponibilidad del campus, como sobre el restablecimiento del servicio. La elección de la(s) acción(es) a ejecutar dependerá del nivel de impacto y duración estimada del incidente, de acuerdo con los siguientes criterios: • Solo acción i) (pieza gráfica): Aplica cuando la indisponibilidad sea visible públicamente (por ejemplo, caída total del campus virtual) y no interfiere con fechas críticas para la inscripción o finalización de los cursos virtuales. • Solo acción ii) (correo a estudiantes): Aplica cuando la afectación sea temporal (menor a 1 hora) y exclusiva para estudiantes matriculados, sin necesidad de informar al público general. • Ambas acciones: Se aplican de manera obligatoria cuando la interrupción sea superior a 1 hora, afecte el desarrollo normal de cursos o impacte fechas de inscripción o finalización de cursos. Se evidencia mediante la consolidación de un reporte donde se registre el monitoreo permanente del	afectación sea temporal (menor a 1 hora) y exclusiva para estudiantes matriculados, sin necesidad de informar al público general. • Ambas acciones: Se aplican de manera obligatoria cuando la interrupción sea superior a 1 hora, afecte el desarrollo normal de cursos o impacte fechas de inscripción o finalización de cursos. Se evidencia en un Reporte Trimestral del Campus Virtual donde se registre el comportamiento de disponibilidad del campus virtual durante el trimestre, incluyendo el historial de funcionamiento, los incidentes presentados, las acciones de continuidad ejecutadas y las comunicaciones realizadas a usuarios y ciudadanía. En caso que no se materialice el riesgo, se debe entregar un reporte trimestral de revisión del historial de disponibilidad del sistema campus virtual, explicando que todo fluyó normalmente, por lo tanto, no fue necesario generar las alertas respectivas ni la reasignación de recursos, mostrando las capturas de pantalla correspondientes. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales.

comportamiento del campus virtual y la captura de pantalla de la publicación de la pieza gráfica en las páginas web de la SIC y del Campus virtual y captura de pantalla aleatoria de algunos correos enviados a los estudiantes, según sea el caso. En caso de no materializarse el riesgo, se debe evidenciar en un reporte que muestre el correcto funcionamiento del campus durante el periodo. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales.	

3) El proceso CS02 FORMACIÓN cambió la descripción de los controles del riesgo PÉRDIDAD DE DISPONIBILIDAD del Sistema de Certificación de Propiedad Industrial.

Control anterior	Control actual
El servidor público o contratista del Grupo de Trabajo de Formación solicita al Grupo de Servicios Tecnológicos ejecutar los respaldos (backups) de los datos críticos de la aplicación del Sistema de Certificación de Propiedad Industrial, de acuerdo con la periodicidad definida. El seguimiento de la ejecución de los respaldos se realiza de forma mensual por el servidor o contratista del Grupo de Formación, mediante el registro y consolidación de los correos electrónicos enviados por el Grupo de Formación a la Mesa de Servicios, en los cuales se solicita el backup correspondiente. Asimismo, se debe conservar la respuesta de la Mesa de Servicios que incluya el reporte del backup realizado. Al final de cada trimestre, se consolidarán los registros correspondientes a los tres respaldos mensuales del periodo, como evidencia	El servidor público o contratista del Grupo de Trabajo de Formación solicita al Grupo de Servicios Tecnológicos ejecutar los respaldos (backups) de los datos críticos de la aplicación del Sistema de Certificación de Propiedad Industrial, de acuerdo con la periodicidad definida. El seguimiento de la ejecución de los respaldos se realiza de forma mensual por el servidor o contratista del Grupo de Formación, mediante el registro y consolidación de los correos electrónicos enviados por el Grupo de Formación a la Mesa de Servicios o el caso creado directamente en la herramienta de help desk de la entidad, con el aval de la Coordinación del Grupo de Trabajo de Sistemas de Información, en los cuales se solicita el backup correspondiente. Asimismo, se debe conservar la respuesta de la Mesa de Servicios que incluya el

de cumplimiento del control y para su inclusión en los informes de seguimiento de la seguridad de la información. Esta actividad se encuentra relacionada con el documento CS02-P04 – Procedimiento para el desarrollo, optimización e implementación de cursos virtuales.	reporte del backup realizado. Al final de cada trimestre, se consolidarán los registros correspondientes a los tres respaldos mensuales del periodo, como evidencia de cumplimiento del control y para su inclusión en los informes de seguimiento de la seguridad de la información. Esta actividad se encuentra relacionada con el documento CS02-P04 – Procedimiento para el desarrollo, optimización e implementación de cursos virtuales.

Control anterior	**Control actual**
En el evento que se presente una falla en el sistema, el Coordinador del Grupo de Trabajo de Formación asignará a un funcionario o contratista para apoyar en el envío de los certificados de participación, de forma manual a los asistentes de los ciclos de formación de propiedad industrial, dentro de los plazos establecidos, a través de la cuenta soportecampusvirtual@sic.gov.co y posteriormente realizará un monitoreo para cerciorarse de que todos los certificados fueron entregados. En caso de rebotar el correo, hacer contacto por otro canal, de acuerdo con el procedimiento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales. Se evidencia trimestralmente mediante la consolidación de un reporte corto donde se registren los correos electrónicos del encargado del envío de los certificados, y el reporte cuantitativo de la gestión realizada. Recopilar las evidencias de la gestión mensual para elaborar el reporte trimestral. Si no se materializa el riesgo, se debe enviar la evidencia mostrando el perfecto funcionamiento del sistema e	En el evento que se presente una falla en el sistema, el Coordinador del Grupo de Trabajo de Formación asignará a un funcionario o contratista para apoyar en el envío de los certificados de participación, de forma manual a los asistentes de los ciclos de formación de propiedad industrial, dentro de los plazos establecidos, a través de la cuenta soportecampusvirtual@sic.gov.co y posteriormente realizará un monitoreo para cerciorarse de que todos los certificados fueron entregados. En caso de rebotar el correo, hacer contacto por otro canal, de acuerdo con el procedimiento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales. Se evidencia trimestralmente mediante la consolidación de un reporte corto donde se registren los correos electrónicos del encargado del envío de los certificados, y el reporte cuantitativo de la gestión realizada. Recopilar las evidencias de la gestión mensual para elaborar el reporte trimestral. Si no se materializa el riesgo, se debe enviar la evidencia mostrando el perfecto funcionamiento del sistema e informando que no fue necesario mandar

informando que no fue necesario mandar los certificados manualmente.	los certificados manualmente. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales.

Se eliminó el siguiente control:

Control eliminado
Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.3 Reporte de debilidades de seguridad de la información. El servidor público o contratista del Grupo de Trabajo de Formación realizará el monitoreo permanente del Sistema de Certificación de Propiedad Industrial, a través de actividades de verificación y validación de funciones a nivel de aplicación. Cuando se detecte una falla en el Sistema de Certificación de Propiedad Industrial, se debe reportar a través de correo electrónico a la mesa de servicios de la entidad, con las evidencias del incidente, para su gestión y solución. Se encuentra relacionado con el documento CS02-P04 Procedimiento para el desarrollo, optimización e implementación de cursos virtuales. Se evidencia en un reporte semestral que contenga el correo enviado por el Grupo de Trabajo de Formación al correo de la mesa de servicios de la entidad. Si no se materializa el riesgo, se debe enviar la misma evidencia mostrando el perfecto funcionamiento del sistema e informando que no fue necesario enviar correos.

4) El proceso CI01 ASESORÍA Y EVALUACIÓN INDEPENDIENTE, cambió el riesgo, la descripción y los controles:

Riesgo anterior	**Riesgo actual**
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).	PÉRDIDAD DE CONFIDENCIALIDAD de la información asociada a la ejecución del Plan Anual de Auditoría (papeles de trabajo, informe preliminar, informe final, entre otros).

Descripción anterior	Descripción actual
Posibilidad de afectación reputacional por reprocesos e incumplimiento en la gestión de la OCI debido la perdida de disponibilidad de los documentos asociados a la ejecución del Plan Anual de Auditoría.	Posibilidad de afectación reputacional por pérdida de seguridad y confidencialidad de la información producida o recibida en la OCI o que se encuentra bajo su responsabilidad, debido al incumplimiento de las políticas de gestión documental y las políticas de seguridad de la información establecidas a nivel institucional.

Control anterior	Control actual
Dominio: A.9 Control de acceso Objetivo: A.9.2 Gestión de acceso de usuarios Control: A.9.2.2 Suministro de acceso de usuarios. El funcionario o contratista de la Oficina de Control Interno administrador de la carpeta digital, donde se almacena la información y evidencias de la ejecución del Plan Anual de Auditorías, el cual ha sido asignado teniendo en cuenta el procedimiento CI01-P02 Auditorías de Control Interno, semestralmente se encargará de verificar que los perfiles y permisos de acceso a la carpeta digital estén actualizados, en caso de detectar algún error en los permisos de acceso o que algún documento ha sido modificado, se socializará la situación en el comité de gestión de la oficina para corregir el permiso de acceso o la modificación de documentos en caso de ser pertinente. La evidencia del control se mostrará por medio del acta del comité.	Dominio: A.9 Control de acceso. Objetivo: A.9.2 Gestión de acceso de usuarios. Control: A.9.2.2 Suministro de acceso de usuarios. El administrador del SharePoint de la OCI será responsable de gestionar los accesos a la carpeta destinada a la Oficina, asignando los permisos y roles adecuados a cada funcionario o contratista, conforme a sus responsabilidades y de acuerdo con el principio de mínimo privilegio. Esta asignación se realizará cada vez que se requiera, asegurando que el acceso a la información almacenada y su respectivo cargue se realice de manera controlada. En caso de detectar accesos no autorizados o comportamientos anómalos en el uso del repositorio, el administrador deberá reportar inmediatamente el incidente a la mesa de servicio y proceder con la revocación o ajuste de los permisos involucrados, conforme a los protocolos establecidos por la entidad. La evidencia de este control será el reporte generado desde la plataforma SharePoint, en el que se consignan los movimientos, accesos y modificaciones realizadas por los diferentes usuarios. Este seguimiento se realizará conforme a lo dispuesto en el

	Procedimiento de Auditorías Internas de Gestión – CI01-P02.

Se eliminó el siguiente control preventivo:

Control eliminado
Dominio: A.12. Seguridad de las operaciones Objetivo: A.12.1 Procedimientos operacionales y responsabilidad Control: A.12.1.1 Procedimientos de operación documentados. Los funcionarios o contratistas asignados como líderes de auditoría o responsables de la elaboración de un informe de ley/seguimiento mensualmente almacenaran los documentos y evidencias de la ejecución del Plan Anual de Auditorías en la carpeta digital de la Oficina de Control Interno teniendo en cuenta la TRD, lo anterior se encuentra documentado en las actividades descritas en el procedimiento CI01-P02 Auditorías de Control Interno, etapa 6 Comunicación de resultados-informe de auditoría, literal j. archivar los soportes de auditoría. La secretaria de la Oficina verificará trimestralmente que el almacenamiento se encuentra completo de acuerdo con lo programado en el Plan Anual de Auditoría, en caso de detectar que no se está realizando el adecuado almacenamiento de la información, informará en el comité mensual de gestión fijando el compromiso y la fecha límite en la que deberá realizarse la actividad. La evidencia del control se mostrará por medio del acta del comité.

Se crearon los siguientes controles preventivos:

Control actual
Dominio: A.8. Gestión de activos. Objetivo: A.8.2 Clasificación de la información. Control: A.8.2.2 Etiquetado de la información. La Secretaría de la OCI realiza anualmente la organización y clasificación de los documentos generados por la Oficina, de acuerdo con la Tabla de Retención Documental (TRD) vigente. Como parte de este proceso, se aplican etiquetas de confidencialidad (confidencial, restringido, interno) a los documentos, con el fin de garantizar su protección y manejo adecuado durante el almacenamiento, uso y transferencia. Posteriormente, la Secretaría socializa en el Comité de Gestión de la Oficina el Formato Único de Inventario Documental (FUID) como constancia de la transferencia documental realizada, conforme al cronograma establecido mediante circular interna de la Entidad. La evidencia del control es el formato FUID (GD01-F01), debidamente diligenciado con la información producida por la OCI durante la vigencia a transferir, en cumplimiento del Procedimiento GD01-P01 de Archivo y Retención Documental.

Control actual
Dominio: A.18. Cumplimiento. Objetivo: A.18.2. Revisiones de seguridad de la información Control: A.18.2.2. Cumplimiento con las políticas y normas de seguridad. La Secretaria de la OCI realiza de manera mensual el seguimiento de la información en el SharePoint de la Oficina, tomando como base el formato CI01F10 Lista de chequeo, en el cual indica si alguno de los documentos incluidos es de carácter confidencial; esto para las Auditorías Internas. La evidencia del control es el formato CI01-F10 y correo electrónico enviado al grupo de trabajo, conforme a lo establecido en el Procedimiento Auditorías Internas de Gestión CI01-P02.

Se definieron 3 nuevas actividades:

Actividad	**Producto esperado**
Realizar capacitación con la OTI para el manejo del Share Point desde rol de administrador, con el fin de dar los accesos correspondientes a la carpeta de la Oficina a los diferentes usuarios, definiendo los perfiles para el manejo de la herramienta.	Listado de perfiles de la herramienta. Lista de asistencia.
Presentar anualmente, en el Comité de Gestión de la Oficina de Control Interno, el estado del archivo de gestión de la OCI frente a los parámetros establecidos en la TRD de la dependencia, así como en los procedimientos y políticas de gestión documental de la entidad.	Formato único de Inventario Documental FUID Acta de Comité de Gestión.
Efectuar la verificación de los documentos producidos en las diferentes auditorías realizadas por la OCI según el PAA de la vigencia, a través del formato CI01F10 Lista de chequeo, registrando en la casilla de observaciones si alguno es de carácter confidencial.	Formato CI01F10 Lista de chequeo diligenciado.

Se eliminaron las siguientes actividades:

Actividad	**Producto esperado**
Solicitar al GGDA capacitación sobre Integridad de la información y la etapa de préstamo de expediente del proceso de Gestión Documental para actualizar el conocimiento del equipo auditor.	Realizar análisis a la necesidad de actualizar la matriz de riesgos de gestión y corrupción del proceso a cargo de la OCI.

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.

5) El proceso GF02 PRESUPUESTAL ajustó la descripción del control correctivo del riesgo: Pérdida de integridad de la información financiera relacionada con los Registro Presupuestales en medio digital (Onedrive).

Control actual
Dominio: A.12 Seguridad en las operaciones Objetivo: A.12.3 Copias de respaldo Control: A.12.3.1 Copias de seguridad de la información. El servidor público de la dirección financiera de presupuesto, en caso de pérdida de integridad debe iniciar la reconstrucción de información a partir de lo cargado en SECOP y SIIF. La evidencia de ejecución del control sería la información de SIIF y SECOP y la información reconstruida.

6) El proceso GA01 SERVICIOS ADMINISTRATIVOS ajustó la descripción de los controles preventivos del riesgo: pérdida de integridad de la información institucional ante accesos no autorizados a la Entidad.

Controles anteriores	**Controles actuales**
Dominio: A.15 Relaciones con los proveedores Objetivo: A.15.2 Gestión de la prestación de servicios de proveedores. Control: 15.2.1 Seguimiento y revisión de los servicios de los proveedores. El servidor público y/o contratista del grupo de trabajo de Servicios Administrativos y Recursos Físicos, constantemente a través de la empresa de vigilancia y seguridad privada administra el circuito cerrado de televisión. En caso de evidenciar un acceso no autorizado, se verificará a través de la video vigilancia y se realizará	Dominio: A.15 Relaciones con los proveedores. Objetivo: A.15.2 Gestión de la prestación de servicios de proveedores. Control: 15.2.1 Seguimiento y revisión de los servicios de los proveedores. El servidor público y/o contratista del grupo de Servicios Administrativos y Recursos Físicos verifica que el contratista que presta el servicio de vigilancia y seguridad privada cumpla con la obligación de supervisión continua y efectiva de las instalaciones de la SIC mediante el sistema de videovigilancia, así como asegurar la comunicación

las investigaciones a que haya lugar, dando aviso al ente competente. La ejecución del control se evidencia a través de los videos de vigilancia. Se encuentra documentado en el procedimiento servicios administrativos GA03-P01.	inmediata y eficaz de cualquier novedad al personal del contratista ubicado en los diferentes pisos de la entidad. De presentarse alguna novedad deberá registrar cualquier novedad o situación sospechosa detectada durante la vigilancia; informar de manera inmediata al personal del CONTRATISTA asignado en los pisos correspondientes, utilizando los canales de comunicación previamente establecidos (radio, teléfono interno, sistema de mensajería u otro medio autorizado). Debe documentar las novedades reportadas, incluyendo hora, ubicación, descripción de la situación y acción tomada; Verificar la atención oportuna y cierre de las novedades comunicadas. De acuerdo con lo establecido en el numeral 7.5.8 del procedimiento GA03-P01.
Dominio: A.11 Seguridad física y del entorno. Objetivo: A.11.1 Áreas seguras. Control: A.11.1.2 Controles de acceso físicos. El servidor público y/o contratista del grupo de trabajo de Servicios Administrativos y Recursos Físicos, permanentemente cuenta con el servicio de vigilancia y seguridad privada, quien verifica que el funcionario o contratista porte el carné para el acceso a las áreas. En caso de no poseer el carné ni tarjeta de acceso, debe registrarse en el libro de registro con el vigilante. En caso de requerirse el ingreso a las instalaciones, se debe solicitar el permiso a través de la herramienta Aranda. La ejecución del control se evidencia a través de los libros de registro, los videos de vigilancia, correos electrónicos y los registro en la herramienta Aranda. Se encuentra documentado en el procedimiento servicios administrativos GA03-P01, y en el contrato de vigilancia.	Dominio: A.11 Seguridad física y del entorno. Objetivo: A.11.1 Áreas seguras. Control: A.11.1.2 Controles de acceso físicos. El acceso a las áreas seguras está controlado por el personal del servicio de vigilancia y seguridad privada, contratado por la entidad. Este personal es responsable de verificar que cada servidor público o contratista porte su carné institucional o tarjeta de acceso como requisito para ingresar a las instalaciones. En caso de que una persona no cuente con su carné o tarjeta de acceso, el ingreso debe registrarse en el libro de control físico, bajo supervisión del personal de vigilancia. Si se requiere el ingreso sin estos elementos, deberá solicitarse un permiso a través de la herramienta Aranda. La ejecución del control queda evidenciada mediante: • Libros físicos de registro de ingreso. • Grabaciones del sistema de videovigilancia. • Correos electrónicos relacionados con solicitudes

	de acceso. • Registros en la herramienta Aranda. Este control se encuentra documentado en el procedimiento GA03-P01 Servicios Administrativos, así como en el contrato de vigilancia vigente.
Dominio: A.9 Control de acceso. Objetivo: A.9.2 Gestión de acceso de usuarios. Control: A.9.2.2 Suministro de acceso de usuarios. El servidor público y/o contratista del grupo de trabajo de Servicios Administrativos y Recursos Físicos encargado de supervisar el contrato mensualmente supervisa el contrato de la empresa de vigilancia y seguridad privada. En caso de encontrar alertas a la ejecución del contrato las comunica al contratista, y/o en caso de requerirse, se da aviso de un posible incumplimiento al grupo de Contratación. La ejecución del control se evidencia a través del contrato con el servicio de vigilancia y seguridad privada; los informes mensuales de ejecución del contrato; comunicación al grupo de contratación, y los correos electrónicos al contratista. Se encuentra documentado en el Manual de contratación - GA01-I02, Formato informe de supervisión y/o cumplimiento a satisfacción del contrato o convenio solicitud y autorización de pago GA01-F08, Procedimiento de etapa de ejecución- GA01-P05.	Dominio: A.9 Control de acceso. Objetivo: A.9.2 Gestión de acceso de usuarios. Control: A.9.2.2 Suministro de acceso de usuarios. El servidor público y/o contratista del grupo de trabajo de Servicios Administrativos y Recursos Físicos, responsable de la supervisión mensual del contrato, realiza el seguimiento a la empresa de vigilancia y seguridad privada. En caso de detectar alertas relacionadas con la ejecución del contrato, estas son comunicadas al contratista. Si se considera necesario, también se informa al grupo de Contratación sobre un posible incumplimiento. La evidencia de la ejecución de este control incluye: • El contrato suscrito con la empresa de vigilancia y seguridad privada. • Informes mensuales de ejecución del contrato. • Comunicaciones enviadas al grupo de Contratación. • Correos electrónicos dirigidos al contratista. Este control se encuentra documentado en los siguientes instrumentos: • Manual de Contratación (GA01-I02). • Formato de informe de supervisión y/o cumplimiento a satisfacción del contrato o convenio: Solicitud y autorización de pago (GA01-F08). • Procedimiento de la etapa de ejecución (GA01-P05).
Dominio: A.7. Seguridad del recurso humano. Objetivo: A. 7.2 Durante la ejecución del empleo. Control: A.7.2.1 Responsabilidades de la dirección. El servidor público y/o contratista del grupo de trabajo de Servicios Administrativos y Recursos Físicos cada vez que se requiera expide o repone el	Dominio: A.7. Seguridad del recurso humano. Objetivo: A. 7.2 Durante la ejecución del empleo. Control: A.7.2.1 Responsabilidades de la dirección. El servidor público y/o contratista del Grupo de Trabajo de Servicios Administrativos y Recursos Físicos es responsable de expedir o reponer el carné

carné institucional y asigna la tarjeta de acceso al funcionario y/o contratista solicitante, con los cuales tendrá acceso a los diferentes pisos de la SIC. En caso de no poseer el carné ni tarjeta de acceso, debe registrarse en el libro de registro con el vigilante. La evidencia de ejecución del control son los registros de solicitudes en la herramienta Aranda, Formatos Solicitud de acceso GA03-F06 diligenciados, Formatos Control de entrega y/o recepción de carné y tarjeta de acceso GA03-F15 diligenciados, y Correos electrónico informando la respuesta a la solicitud. Se encuentra documentado en el procedimiento servicios administrativos GA03-P01.	institucional y asignar la tarjeta de acceso al funcionario y/o contratista solicitante, cada vez que se requiera. Estos elementos permiten el ingreso a los diferentes pisos de la SIC. En caso de no contar con el carné ni con la tarjeta de acceso, el ingreso deberá registrarse manualmente en el libro de control en poder del personal de vigilancia. Las evidencias de la ejecución de este control incluyen: • Registros de solicitudes en la herramienta Aranda. • Formato GA03-F06 - Solicitud de acceso debidamente diligenciado. • Formato GA03-F15 - Control de entrega y/o recepción de carné y tarjeta de acceso, debidamente diligenciado. • Correos electrónicos con la respuesta formal a la solicitud. Este control se encuentra documentado en el procedimiento GA03-P01 - Servicios Administrativos.

7) El proceso GA02 INVENTARIOS ajustó la descripción de los controles preventivos del riesgo pérdida de integridad durante la gestión de la información de los inventarios en Helisa.

Controles anteriores	**Controles actuales**
Dominio: A.9 Control de acceso. Objetivo: A.9.2 Gestión de acceso de usuarios. Control: A.9.2.2 Suministro de acceso de usuarios. El servidor público y/o contratista del grupo de Trabajo Servicios Administrativos y Recursos Físicos cada vez que se requiera, genera usuarios y permisos de acceso al hosting del aplicativo de inventarios Helisa. A través de la plataforma web de Proasistemas se solicita el soporte técnico para servicios en la nube, cada vez que se presenta una falla de acceso al hosting. La ejecución del control se evidencia a través de correos electrónicos. Se encuentra	Dominio: A.9 Control de acceso. Objetivo: A.9.2 Gestión de acceso de usuarios. Control: A.9.2.2 Suministro de acceso de usuarios. El personal autorizado del Grupo de Trabajo de Servicios Administrativos y Recursos Físicos (servidores públicos y/o contratistas) gestiona la creación de usuarios y la asignación de permisos de acceso al entorno de hosting del aplicativo de inventarios Helisa, según las necesidades operativas. Cuando se presentan incidencias de acceso, se realiza una solicitud de soporte técnico a través de la plataforma web de Proasistemas, proveedor del servicio en la

documentado en el Instructivo de Acceso a Helisa Cloud y Hosting del Departamento de Tecnología (documento del proveedor).	nube. La evidencia de ejecución del control se conserva en registros de correo electrónico. El procedimiento se encuentra descrito en el Instructivo de Acceso a Helisa Cloud y Hosting, documento del proveedor administrado por el Departamento de Tecnología.
Dominio: A.12 Seguridad de las operaciones. Objetivo: A.12.1 Procedimientos operacionales y responsabilidades. Control: A.12.1.1 Procedimientos de operación documentados. El servidor público y/o contratista del grupo de Trabajo Servicios Administrativos y Recursos Físicos cada vez que se requiera, socializa los videos tutoriales y/o se presenta el programa de capacitación proporcionado por el proveedor del aplicativo de inventarios. Cuando haya inquietudes, se consulta los videos tutoriales para su aclaración. La ejecución del control se evidencia a través de los videos tutoriales y el Programa de capacitación proporcionados por el proveedor; la socialización de los videos a los integrantes del grupo de trabajo y los certificados de la capacitación. Se encuentra documentado en el programa de capacitación.	Dominio: A.12 Seguridad de las operaciones. Objetivo: A.12.1 Procedimientos operacionales y responsabilidades. Control: A.12.1.1 Procedimientos de operación documentados. El personal del Grupo de Trabajo de Servicios Administrativos y Recursos Físicos ya sea servidor público o contratista, realiza la socialización interna del programa de capacitación y los videos tutoriales proporcionados por el proveedor del aplicativo de inventarios Helisa, cada vez que se requiere fortalecer el conocimiento operativo sobre el sistema. Ante dudas o incidencias operativas, se recurre a estos recursos audiovisuales como guía de referencia. La ejecución del control se evidencia mediante los siguientes elementos: • Videos tutoriales y programa de capacitación entregados por el proveedor • Registro de socialización interna con el equipo de trabajo • Certificados de participación en las capacitaciones Este procedimiento se encuentra documentado en el Programa de Capacitación del proveedor y es gestionado por el Departamento de Tecnología.

Dominio: A.9 Control de acceso. Objetivo: A.9.2 Gestión de acceso de usuarios. Control: A.9.2.2 Suministro de acceso de usuarios. El servidor público y/o contratista del grupo de Trabajo Servicios Administrativos y Recursos Físicos cada vez que se requiera, genera usuarios, permisos de acceso y asignación de roles a los usuarios autorizados al aplicativo de inventarios Helisa. Cuando exista un cambio de administrador se informa al proveedor para que genere el cambio en el aplicativo. Cuando exista cambios en los otros roles, debe informarse al administrador para que realice los ajustes en el aplicativo. La ejecución del control se evidencia a través de correos electrónicos.	Dominio: A.9 Control de acceso. Objetivo: A.9.2 Gestión de acceso de usuarios. Control: A.9.2.2 Suministro de acceso de usuarios. El personal autorizado del Grupo de Trabajo de Servicios Administrativos y Recursos Físicos (servidores públicos y/o contratistas) gestiona la creación de usuarios, la asignación de permisos de acceso y la definición de roles para el uso del aplicativo de inventarios Helisa. Cuando se produce un cambio en el rol de administrador, se notifica al proveedor del sistema para que realice la actualización correspondiente. En el caso de cambios en otros roles, estos deben ser informados al administrador del sistema Helisa para su ajuste dentro del aplicativo. La ejecución del control se respalda mediante evidencia documental, como correos electrónicos que registran las solicitudes y confirmaciones de los cambios realizados.

Dominio: A.16. Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.2 Reporte de eventos de seguridad de la información. El servidor público y/o contratista del grupo de Trabajo Servicios Administrativos y Recursos Físicos cada vez que se requiera, documenta la inconsistencia presentada en el aplicativo de inventarios para que el proveedor brinde el soporte técnico necesario. En caso de requerirse un ajuste al aplicativo, se realizan mesas con el grupo de trabajo y se le indica al proveedor los ajustes requeridos al aplicativo. La ejecución del control se evidencia a través de correos electrónicos o mediante la comunicación por el sistema de trámites. Se encuentra documentado en el contrato del proveedor.	Dominio: A.16. Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.2 Reporte de eventos de seguridad de la información. Cuando se presenta una inconsistencia o evento relacionado con la seguridad de la información en el aplicativo de inventarios Helisa, el personal del Grupo de Trabajo de Servicios Administrativos y Recursos Físicos (servidores públicos y/o contratistas) documenta el incidente y notifica al proveedor para que brinde el soporte técnico correspondiente. En los casos que requieren ajustes estructurales o funcionales al aplicativo, se llevan a cabo reuniones técnicas con el equipo de trabajo, en las cuales se definen los cambios necesarios y se comunican formalmente al proveedor. La ejecución de este control se evidencia a través de los registros de correo electrónico o por medio de las comunicaciones enviadas mediante el sistema institucional de trámites. Este procedimiento se encuentra respaldado en el contrato suscrito con el proveedor del servicio.

8) El proceso CS0CS05 GESTIÓN INTEGRAL DE DATOS PERSONALES creó dos riesgos de seguridad de la información ante la pérdida de integridad.

Riesgo no.1	**Descripción**
Pérdida de integridad por la modificación no autorizada de datos personales en el sistema de trámites.	Posibilidad de afectación reputacional por pérdida de credibilidad y confianza de los ciudadanos, grupos de valor y partes interesadas, debido a modificaciones no autorizadas de datos personales en el sistema de trámites.

Riesgo no.2	Descripción
Pérdida de integridad durante la gestión de la tabla de control de reclamos y consultas del proceso.	Posibilidad de afectación reputacional por pérdida de credibilidad y confianza de los ciudadanos, grupos de valor y partes interesadas, debido a errores en la tabla de control de reclamos y consultas del proceso.

Los siguientes son los controles preventivos establecidos:

Riesgo	Control
No.1	Dominio: 12. Seguridad de las operaciones. Objetivo: 12.1 Procedimientos operacionales y responsabilidades. Control: 12.1.1 Procedimientos de operación documentados. El contratista de la Oficina Asesora de Planeación, en su calidad de apoyo jurídico de la Oficial de Protección de Datos Personales, diligencia semanalmente una matriz de control en la que se registran los reclamos relacionados con la actualización y corrección de datos personales. La información que alimenta dicha matriz proviene del sistema de trámites. En ella se consignan, entre otros aspectos, el número de radicado de cada petición, la fecha de ingreso, la tipología del reclamo, la identificación del usuario, la descripción de la solicitud y la fecha en que las peticiones son remitidas a la Oficina de Tecnologías de la Información (OTI) para la realización de los ajustes correspondientes. La remisión de estas solicitudes se efectúa mediante correo electrónico enviado por el contratista a la OTI. Asimismo, la matriz incluye la fecha en que se brinda respuesta al usuario y se gestiona desde la carpeta compartida de la Oficina Asesora de Planeación, ubicada en la carpeta Oficial de Protección de Datos Personales.

Riesgo	Controles
No.2	Dominio: 9. Control de acceso. Objetivo: 9.2 Gestión de acceso de usuarios. Control: 9.2.2 Suministro de acceso de usuarios. El profesional designado de la OAP y el contratista (apoyo jurídico de la Oficial de Protección de Datos Personales), de manera permanente son los colaboradores que tienen acceso y permisos diferenciados para la edición de la tabla de control de reclamos y consultas del proceso. El profesional designado de la OAP, consolida y carga la versión de la matriz actualizada, semanalmente. La evidencia de ejecución del control se encuentra dispuesta en la carpeta compartida de la OAP.
	Dominio: 18. Cumplimiento. Objetivo: 18.1 Cumplimiento de requisitos legales y contractuales. Control: 18.1.3 Protección de registros.

	El profesional designado de la OAP semanalmente debe verificar la consistencia de la última versión de la tabla de control de reclamos y consultas del proceso, con el sistema de trámites, contrastando salidas (respuestas enviadas) con los registros del sistema. En caso de encontrar inconsistencias, el profesional debe informar los errores al contratista (apoyo jurídico de la Oficial de Protección de Datos Personales), para que realice los ajustes. La evidencia de ejecución del control se encuentra dispuesta en la carpeta compartida de la OAP.

9) El proceso CS01 SERVICIO A LA CIUDADANÍA realizó ajustes al riesgo de disponibilidad, la descripción y los controles.

Riesgo anterior	**Riesgo actual**
PÉRDIDAD DE DISPONIBILIDAD de la funcionalidad de los canales de atención virtuales (SIC Facilita), formulario en línea de PQR, ocasionando indisponibilidad de la información generada por el ciudadano y fallas de las herramientas tecnológicas que permiten gestionar los derechos de petición.	PÉRDIDAD DE DISPONIBILIDAD de la funcionalidad de los canales de atención virtuales (SIC Facilita), formulario en línea de PQRSF y Sistema de Trámites, ocasionando indisponibilidad de la información generada por el ciudadano y fallas de las herramientas tecnológicas que permiten gestionar los derechos de petición.

Descripción anterior	**Descripción actual**
Posibilidad de afectación reputacional por quejas y reclamos de las partes interesadas por indisponibilidad prolongada, así como del Sistema de Trámites de la entidad impidiendo la gestión oportuna de los derechos de petición y de SIC Facilita debido a fallas en la infraestructura tecnológica de la SIC.	Posibilidad de afectación reputacional por quejas y reclamos de las partes interesadas por indisponibilidad prolongada del formulario web de radicación de PQRSF, así como del Sistema de Trámites de la entidad impidiendo la gestión oportuna de los derechos de petición y de SIC Facilita debido a fallas en la infraestructura tecnológica de la SIC.

Eliminó el siguiente control tipo preventivo:

Control eliminado
Dominio: A.12 Seguridad de las operaciones. Objetivo: A.12.4 Registro y seguimiento. Control: A.12.4.1 Registro de eventos.

El Coordinador del grupo de Trabajo de Atención al Ciudadano revisa el resultado del monitoreo diario sobre la disponibilidad de los canales de atención, del Sistema de trámites y las pruebas de funcionamiento previa al inicio de actividades diarias, entregado por el proveedor de los servicios de BPO. En caso de encontrar novedades con el acceso al Sistema de trámites por fallas en la conexión de internet o en las lupas de validación, se reporta de inmediato al Grupo de Servicios Tecnológicos para que procedan con las acciones de restablecimiento de los sistemas. La evidencia de ejecución del control es el registro de la novedad presentada ante Mesa de servicios.

Se ajustó el control tipo detectivo:

Control anterior	**Control actual**
Dominio: A.16 Gestión de incidentes de seguridad de la información Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información Control: A. 16.1.5 Respuesta a incidentes de seguridad de la información. El Servidor público o contratista del Grupo de Servicios Tecnológicos cuando se requiera, realiza el diagnóstico ante la falla presentada. Cuando se detecte indisponibilidad de los sistemas, toma las acciones requeridas para habilitar nuevamente el sistema. Como evidencia se cuenta con los reportes generados. Se encuentra relacionado en la documentación de la Mesa de Servicios Tecnológicos. Se cuenta con el procedimiento de Gestión de incidentes SC05-P01; procedimiento Gestión de disponibilidad GS01-P22.	Dominio: A.16 Gestión de incidentes de seguridad de la información Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información Control: A. 16.1.5 Respuesta a incidentes de seguridad de la información. El Servidor público o contratista del Grupo de Servicios Tecnológicos cuando se requiera, realiza el diagnóstico ante la falla presentada. Cuando se detecte indisponibilidad de los sistemas, toma las acciones requeridas para habilitar nuevamente el sistema. Como evidencia se cuenta con los reportes generados. Se encuentra relacionado en la documentación de la Mesa de Servicios Tecnológicos. Se cuenta con el Procedimiento GS01-P13 – Gestión de Incidentes TI.; procedimiento Gestión de disponibilidad GS01-P22.

Creó el siguiente control tipo correctivo:

Nuevo control
Dominio: A.16 Gestión de incidentes de seguridad de la información. Objetivo: A.16.1 Gestión de incidentes y mejoras en la seguridad de la información. Control: A.16.1.2 Reporte de eventos de seguridad de la información. El servidor público o contratista del Grupo de Trabajo de Atención al Ciudadano encargado del proceso SIC Facilita debe informar cada vez que se presenten incidentes tecnológicos en la plataforma SIC FACILTA a la Oficina de Tecnología e Informática de la SIC. Si se confirma por parte de la OTI que el incidente que se

presenta no es de solución inmediata o que este tarda un tiempo considerable en ser resuelto, el servidor público o contratista del Grupo de Trabajo de Atención al Ciudadano contacta por correo electrónico o llamada telefónica a los proveedores vinculados a la plataforma y a los consumidores para informarles si procede la reprogramación de los chats de facilitación. La evidencia de ejecución del control es el registro en el Sistema de trámites con la actuación "Comunicación". De acuerdo con lo establecido en el CS01-P01 PROCEDIMIENTO SIC FACILITA.

Se definieron nuevas actividades:

Actividad	Producto esperado
Publicar en el banner de la Sede Electrónica un aviso de indisponibilidad de los aplicativos cuando sea necesario y, si aplica, los medios alternativos para trámites o consultas para asegurar una adecuada información a la ciudadanía.	Registro de publicaciones en Sede Electrónica.
Analizar la viabilidad de utilizar Microsoft Teams para realizar los chats de mediación en los casos en donde no se tenga disponibilidad de la plataforma institucional.	Documento resultado análisis de viabilidad.

Se eliminó la siguiente actividad:

Actividad	Producto esperado
Informar al Grupo de Servicios Tecnológicos las novedades yo incidentes presentados sobre la indisponibilidad del Sistema de trámites y de SICFacilita, formulario en línea de PQRS.	Registro de solicitudes por correo electrónico tickets

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 tercer trimestre se identificaron las siguientes actividades a las cuales se les debería dar cumplimiento:

PROCESO	RIESGO	ACTIVIDAD	PRODUCTO ESPERADO	FECHA FIN	ESTADO
NOTIFICACIONES	PÉRDIDA DE CONFIDENCIALIDAD una indebida notificación a una dirección errónea.	Hacer seguimiento y verificación del funcionamiento adecuado de la planilla electrónica de numeración, y de requerirse corrección de fallas, se solicitará a la OTI para proceder.	Acta de la reunión	31/07/2025	Actividad cumplida por el área.
SERVICIOS ADMINISTRATIVOS	PÉRDIDAD DE INTEGRIDAD - de la información institucional ante accesos no autorizados a la Entidad	Gestionar la capacitación al equipo de trabajo del grupo de SAyRF en las políticas seguridad de la información implementadas por la entidad.	capacitación realizada	31/07/2025	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	31/07/2025	Actividad cumplida por el área.
INVENTARIOS	PÉRDIDA DE INTEGRIDAD durante la gestión de la información de los inventarios en Helisa.	Solicitar una capacitación al proveedor del aplicativo de Inventarios de la Entidad, en cuanto a las políticas de seguridad de la información frente al manejo del mismo.	capacitación realizada	31/07/2025	Actividad cumplida por el área.

PROCESO	RIESGO	ACTIVIDAD	PRODUCTO ESPERADO	FECHA FIN	ESTADO
		Solicitar al proveedor Proasistemas capacitación al personal de almacén sobre el manejo adecuado del aplicativo de inventarios de la Entidad.	capacitación realizada	31/07/2025	Actividad cumplida por el área.
PRESUPUESTAL	PÉRDIDA DE INTEGRIDAD de la información financiera relacionada con los Registro Presupuestales en medio digital (Onedrive).	Solicitar al área de contratos confirmación de los usuarios que deben tener acceso a la carpeta de presupuesto y efectuar una validación de los usuarios actualmente autorizados en el drive para efectuar los ajustes que correspondan-	Correo de solicitud y pantallazo del drive con los permisos ajustados.	16/07/2025	Actividad cumplida por el área.
SERVICIOS ADMINISTRATIVOS	PÉRDIDAD DE INTEGRIDAD de la información institucional ante accesos no autorizados a la Entidad.	Socializar la actualización de la matriz de activos de la información a los funcionarios y Contratistas del grupo de SAyRF.	Socialización realizada.	1/08/2025	Actividad cumplida por el área.
GESTIÓN DOCUMENTAL	PÉRDIDA DE DISPONIBILIDAD de la información institucional en el evento de un traslado o retiro de un funcionario o contratista.	Capacitación en el grupo sobre la importancia de la seguridad de la información y las mejores prácticas de manejo de los documentos.	Material de la capacitación, registro de asistencia a las capacitaciones y evaluación de conocimientos.	29/08/2025	Actividad cumplida por el área.

PROCESO	RIESGO	ACTIVIDAD	PRODUCTO ESPERADO	FECHA FIN	ESTADO
TRAMITES ADMINISTRATIVOS - PROTECCIÓN DEL CONSUMIDOR	PÉRDIDA DE DISPONIBILIDAD - ante manejo inadecuado de la información digital.	Solicitar a la OTI capacitación sobre activos de información y seguridad de la información, para el personal de la Dirección y grupos adscritos.	Soporte de asistencia.	30/09/2025	Actividad cumplida por el área.
CONTABLE	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 contables.	Realizar mesa de trabajo entre la Dirección Financiera y la OTI para verificar el periodo de retención de los bakcups diarios con relación al espacio de almacenamiento y a la operación actual del sistema.	Acta de mesa de trabajo.	30/09/2025	Actividad cumplida por el área.
GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN	PÉRDIDA DE DISPONIBILIDAD por vencimiento y no renovación de licenciamiento de los artefactos de arquitectura empresarial.	Documentar detalladamente lineamientos de uso y actualización de la herramienta de arquitectura disponible.	Documento uso y actualización de herramienta de arquitectura disponible.	30/09/2025	Actividad cumplida por el área.

5. CONCLUSIÓN

En conclusión, se evidencia que cada una de las áreas gestionaron las actividades planeadas a ejecutarse en tercer trimestre: en julio 6 actividades, en agosto 2 actividades y en septiembre 3 actividades.
De conformidad con lo anteriormente descrito, se confirma la ejecución de 11 actividades.

Hasta el segundo trimestre se habían ejecutado dieciséis (16) actividades, pero al eliminar dos riesgos, se eliminaron 2 actividades que habían sido atendidas en marzo de 2025, por lo tanto, hasta el tercer trimestre (30 de septiembre de 2025) se ha dado cumplimiento a 25 actividades. Teniendo en cuenta que se adicionaron nuevas

actividades, actualmente son en total 101 actividades descritas en los planes de tratamiento de riesgos de seguridad de la información. Aplicando la fórmula de la regla de tres simple directa, se evidencia un avance del 24,75%.

Nota: La confirmación de la ejecución de las actividades, se evidencia en la carpeta compartida "*Soportes de los procesos*" 2.1. Soportes de los procesos corte Septiembre.

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