PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

UNIDAD PARA LA VÍCTIMAS

Oficina de Tecnologías de la Información

Tabla de Contenido

1. OBJETIVO

En el presente documento se presentan los planes de tratamiento al riesgo asociado al Sistema de Gestión de Seguridad de la Información (SGSI) para el correspondiente seguimiento y verificación al cumplimiento de los planes definidos en el marco de la metodología para la administración de riesgos establecida por la Unidad para la Víctimas.

2. ALCANCE

En el marco de los planes de tratamiento al riesgo se encuentran actualizados e identificados los riesgos de seguridad de la información.

3. PLANES DE TRATAMIENTO AL RIESGO

Se toma como base el inventario de activos de información realizado Agosto 2023 con el apoyo de los Enlaces del SIG de la Unidad para las Víctimas, en la siguiente grafica se observa el nivel de riesgo residual con corte a Diciembre 2023:

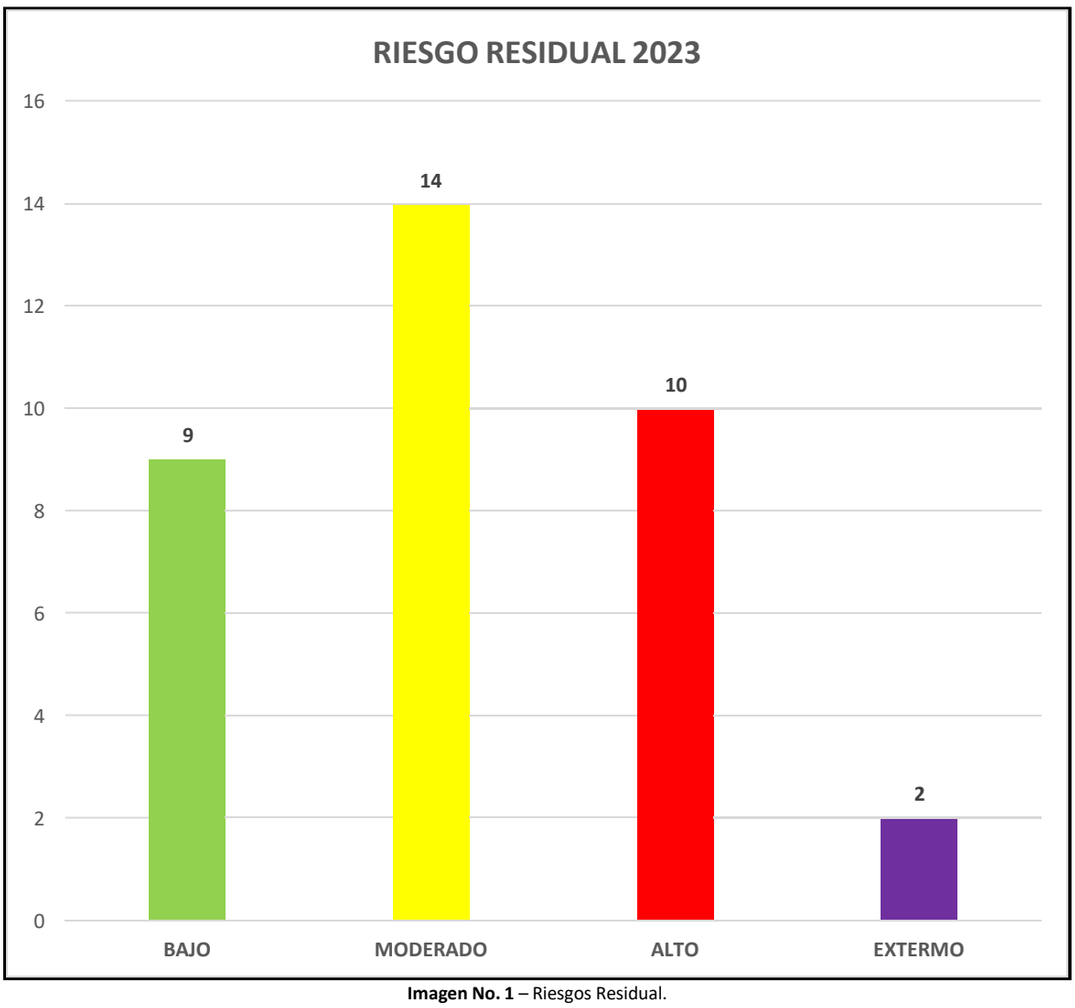

Imagen No. 1 – Riesgos Residual.

No. de Riesgo:	35
No. de Planes de Controles:	81
No. de Planes de Tratamiento:	48

3.1. Riesgos de Gestión Contractual

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Elaborar las minutas de los contratos derivados de los procesos de contratación adelantados por la entidad, de acuerdo a la modalidad de contratación.	Posibilidad de pérdida económica y reputacional por pérdida a la Confidencialidad de la Información de la Entidaddebido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	Baja	Mayor	Alto	El Proceso de Gestión Contractual suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas del Proceso cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de NO contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado . Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión Contractual y/o reporte de dicho registro. **(A.6.6)**	**Alto**	Reducir - Mitigación	El enlace SIG del Proceso de Gestión Contractual deberá socializar los compromisos y estado actual del Sistema de Gestión de Seguridad de la Información (SGSI) de cada uno de los encuentros "Enlace SIG" y retroalimentar la información que es generada por parte de la Oficina de Tecnología de Información (OTI) en materia de Seguridad la cual es publicada en la intranet y promover al interior del Proceso a la participación de las charlas de seguridad convocadas. **Evidencia:** Correo electrónico del resumen de encuentro SIG en materia de Seguridad o correos con infografía publicada. **(A.6.3)**
					El Proceso de Gestión Contractual firma Acuerdo de Confidencialidad con Gestión Documental para el cargue y descarga de expedientes contractuales de la herramienta de ARCHIDU. **Evidencia:** Los Acuerdos de Confidencialidad de ARCHIDU suscritos por el proceso de Gestión Contractual. **(A.6..6)**			El Proceso de Gestión Contractual asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información replicados por el enlace del proceso. **(A.6.3)**
Elaborar las minutas de los contratos derivados de los procesos de contratación adelantados por la entidad, de acuerdo a la modalidad de contratación.	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidaddebido a la falla o ausencia de controles de seguridad aplicables.	Baja	Moderado	Moderado	El Proceso de Gestión Contractual realiza entrega formal de los expedientes físicos al Proceso de Gestión Documental a través de memorando (Radicados). **Evidencia:** Los memorandos (Radicados) al Proceso de Gestión Documental. **(A.5.9, A.5.10, A.5.11)**	**Moderado**	Reducir - Mitigación	El Proceso de Gestión Contractual retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13)**
					El Proceso de Gestión Contractual realiza publicación de la etapa precontractual y post-contractual en el aplicativo SECOP, con el fin de tener la información disponible y actualizada de los procesos ejecutados. **Evidencia:** Se relacionaran los enlaces directos de los procesos ejecutados en el aplicativo SECOP. **(A.8.8)**			

3.2. Riesgos de Gestión de Talento Humano

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Administrar historias laborales y el Sistema Tecnológico KACTUS. Implementar, con el acompañamiento del GGAD, las TRD mediante la elaboración de los inventarios documentales de los archivos de gestión del total de las series y subseries de la TRD de la dependencia. Clasificar, con el acompañamiento del Grupo de Gestión Administrativa y Documental (GGAD) la documentación electrónica o digital bajo la estructura de las TRD (series y subseries) en las herramientas tecnológicas disponibles para tal fin. Participar en las jornadas del plan de capacitación del sistema de gestión documental.	**Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidaddebido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.**	Muy baja	Moderado	Moderado	El Proceso de Gestión Talento Humano suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado . Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión de Talento Humano y/o reporte de dicho registro. **(A.6.6)**	**Moderado**	Aceptar	El Proceso de Gestión de Talento Humano debe notificar a los administradores del sistema de Información KACTUS las novedades de (personal) de los usuarios que hace uso del Sistema de Información. **Evidencia:** Correo Electrónico de notificación. **(A.5.15)**
Administrar historias laborales y el Sistema Tecnológico KACTUS. Implementar, con el acompañamiento del GGAD, las TRD mediante la elaboración de los inventarios documentales de los archivos de gestión del total de las series y subseries de la TRD de la dependencia. Clasificar, con el acompañamiento del Grupo de Gestión Administrativa y Documental (GGAD) la documentación electrónica o digital bajo la estructura de las TRD (series y subseries) en las herramientas tecnológicas disponibles para tal fin. Participar en las jornadas del plan de capacitación del sistema de gestión documental.	**Posibilidad de pérdida económica y reputacional por pérdida a la Integridad de la Información de la Entidaddebido a la falla o ausencia de controles relacionados con el uso adecuado de la información.**	Muy baja	Moderado	Moderado	**El Proceso de Gestión de Talento Humano a través del Técnico y/o Auxiliar Administrativo valida la solicitud de los documentos de las historias laborales y confirma autorización de trámite por la Coordinadora de Talento Humano.** **Solicita la historia laboral al Grupo de Gestión Administrativa y Documental en los formatos respectivos para el préstamo del expediente y de control de los archivos de gestión conforme a las tablas de retención documental.** **En caso de no contar con la información actualizada en la historia laboral se remite correo a la Coordinadora de Talento Humano, con el fin de identificar la solicitud de la historia laboral con los demás líderes de TH.** **Evidencia: Correo electrónico, Hoja De Control Archivos De Gestión y Formato De Préstamo de Documentos Y/O Expedientes.** **[A.6.1, A.6.2, A.6.5, A.5.3, A.5.11, A.7.10, A.5.37]**	**Moderado**	Reducir - Mitigación	El Proceso de Gestión de Talento Humano asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación a la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información replicados por el enlace del proceso. **(A.6.3)**

3.3. Riesgos de Gestión Financiera

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Control y registro de información financiera en SIIF NACION II.	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidaddebido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	Media	Catastrófico	Extremo	El Proceso de Gestión Financiera suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado . Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión de Financiera y/o reporte de dicho registro. **(A.6.6)**	**Extremo**	Reducir - Mitigación	El Proceso de Gestión Financiera notifica a administrador del SIIF de la Entidad y a la Oficina de Tecnología de la Información (OTI) las novedades del funcionario y/o contratista para que se inactive el usuario. En caso de no presentarse novedad el Proceso de Gestión Financiera deberá reportar un correo indicando que no se presento novedades en el período. **Evidencia:** correo de notificación de la novedad para inactivación del acceso a usuario o correo de notificación indicando que no se presento novedades en el período. **(A.6.2, A.6.3, A.6.5, A.6.6)** El Proceso de Gestión Financiera enviara una notificación para que los procesos que interactúan con SIIF reporte novedades de desvinculación. **Evidencia:** Correo o memorando o circular a los procesos que interactúan con SIIF. **(A.6.2, A.6.3, A.6.5, A.6.6)**
Control y registro de información financiera en SIIF NACION II.	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidaddebido a la falla o ausencia de controles de seguridad aplicables.	Alta	Menor	Moderado	El Proceso de Gestión Financiera aplica el formato de responsabilidad de uso de la firma digital por medio de TOKEN el cual es asignado a funcionarios y/o contratistas específicos para la ejecución de las actividades propias del Proceso. **Evidencia:** Diligenciamiento del formato de responsabilidad. **(A.6.6)** El Proceso de Gestión Financiera realiza el control para el préstamo de documentos físicos o digitales del proceso a través de una solicitud por correo electrónico. Para el préstamo de archivos físicos se realiza el envió de correo a Gestión Documental y para el préstamo de archivos digitales (internos) del proceso se realiza la solicitud al profesional o apoyo de archivo de Gestión financiera. **Evidencia:** Envió de la solicitud a través de correo electrónico. **(A.5.2, A.5.3, A.5.4, A.5.10, A.5.11, A.5.15, A.5.33)** El Proceso de Gestión Financiera retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13)**	**Bajo**	Aceptar	N/A

3.4. Riesgos de Gestión Jurídica

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Ejercer la defensa técnica judicial y extrajudicial de la Entidad y realizar el recaudo de las obligaciones y acreencias a favor de la Entidad y Saneamiento de bienes que se encuentran bajo la administración del Fondo de Reparación a las Victimas (FRV).	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	Muy baja	Mayor	Alto	El Proceso de Gestión Jurídica suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado . Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión de Jurídica y/o reporte de dicho registro. **(A.6.6)** El Proceso de Gestión Jurídica notifica al administrador de los Sistemas de Información(LEX) de la Entidad y a la Oficina de Tecnología de la Información (OTI) las novedades del funcionario y/o contratista para que se inactive el usuario. En caso de no presentarse novedad el Proceso de Gestión Financiera deberá reportar un correo indicando que no se presento novedades en el periodo. **Evidencia:** correo de notificación de la novedad para inactivación del acceso al usuario o correo de notificación indicando que no se presento novedades en el período. **(A.6.2, A.6.3, A.6.5, A.6.6)**	**Moderado**	Reducir - Mitigación	El Proceso de Gestión de Jurídica asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información replicados por el enlace del proceso y lista de asistencia. **(A.6.3)**
Ejercer la defensa técnica judicial y extrajudicial de la Entidad y realizar el recaudo de las obligaciones y acreencias a favor de la Entidad y Saneamiento de bienes que se encuentran bajo la administración del Fondo de Reparación a las Victimas (FRV).	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad debido a la falla o ausencia de controles de seguridad aplicables.	Alta	Mayor	Alto	El Proceso de Gestión Jurídica retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13)** El Proceso de Gestión Jurídica aplica control de acceso a los usuarios para (consulta, adición y modificación) de la información en la herramienta de SharePoint. **Evidencia:** Correo de solicitud a la OTI para conocer los permisos asociados al SharePoint del Proceso. **(A.5.2, A.5.3, A.5.15)**	**Alto**	Reducir - Mitigación	El Proceso de Gestión Jurídica realiza mesas de trabajo con la Oficina de Tecnología de la Información (OTI) con el fin de identificar las necesidades o requerimientos para el desarrollo de un Sistema de Información en el que se lleve el registro de los procesos internos de: Grupo de Defensa judicial (Procesos coactivos, contencioso administrativo, Persuasivo, Saneamiento), Grupo Respuesta judicial, Gestión normativa. **Evidencia:** Actas de reunión y listas de asistencia.. **(A.8.26, A.8.29, A.8.31)**

3.5. Riesgos de Control Interno Disciplinario

Adelantar las actuaciones contra los servidores y exservidores públicos de la entidad, originadas con ocasión de una noticia con presunta incidencia disciplinaria, en virtud a una queja, informe, de oficio o anónimo, y finaliza hasta la etapa de instrucción de conformidad con lo establecido en la Ley 1952 de 2019 modificada parcialmente por la Ley 2094 de 2021 (Código General Disciplinario).	**Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.**	Baja	Moderado	Moderado	El Proceso de Control Interno Disciplinario suscribe un "Acuerdo de Confidencialidad" de usuarios de aplicativos, herramientas o información , con cada uno de los funcionarios y/o contratistas del Proceso, para acceder a la información del proceso y de la Entidad, en caso de NO contar con el "Acuerdo", no se asignaran accesos ni usuarios; en los casos en los que se termine la contratación o por renuncia de algún colaborador los usuarios serán deshabilitados. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Control Interno Disciplinario y/o reporte de dicho registro. **(A.6.6)** Los funcionarios y/o contratistas de Proceso de Control Interno Disciplinario, son responsables de salvaguardar la información de los expedientes físicos a su cargo. Cuando alguno de los funcionarios y colaboradores requieran el ingreso al archivo físico, se realizará la solicitud a la persona delegada por el proceso mediante el registro de la planilla de ingreso y/o envío de correo electrónico. En caso de que el usuario no reporte el ingreso al archivo físico, la persona designada enviará correo en el que se recuerde que se debe dar cumplimiento de los lineamientos establecidos al interior del proceso. **Evidencia:** Registro de la planilla de ingreso y/o envío de correo electrónico y/o correos recordatorios de cumplimiento de lineamientos. **(A.7.2)**	**Moderado**	Reducir - Mitigación	Por parte del Coordinador del Grupo de Control Interno Disciplinario se solicitará una reunión para que desde la Oficina de Tecnologías de la Información, se garantice la salvaguarda de la información del proceso, que se encuentra guardada en OneDrive, dentro de la cual se busca contar con niveles de acceso de acuerdo con los roles de los funcionarios del grupo asignados para esto. Adicionalmente, se solicitará a la OTI mapeo de los nombres de las personas que hayan ingresado a OneDrive y que correspondan solamente a funcionarios y colaboradores autorizados del grupo Control Interno Disciplinario. Como evidencia quedará Acta de Reunión y compromisos.
Adelantar las actuaciones contra los servidores y exservidores públicos de la entidad, originadas con ocasión de una noticia con presunta incidencia disciplinaria, en virtud a una queja, informe, de oficio o anónimo, y finaliza hasta la etapa de instrucción de conformidad con lo establecido en la Ley 1952 de 2019 modificada parcialmente por la Ley 2094 de 2021 (Código General Disciplinario).	**Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables.**	Muy baja	Menor	Bajo	El Proceso de Control Interno Disciplinario retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13)**	**Bajo**	Aceptar	N/A

3.6. Riesgos de Gestión para la Asistencia

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Analizar, tramitar las solicitudes y realizar la colocación de recursos a los registros viables por concepto de Atención Humanitaria y Ayuda Humanitaria.	**Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.**	Baja	Moderado	Moderado	El Proceso de Gestión para la Asistencia suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas y/o operador del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión para la asistencia y/o reporte de dicho registro. **(A.6.6)**	**Moderado**	Reducir - Mitigación	El enlace SIG del Proceso de Gestión para la Asistencia socializa la información del Sistema de Gestión de Seguridad de la Información a los funcionarios, contratistas y operadores del proceso cada vez que la Oficina de Tecnología de la Información (OTI) las publique. **Evidencia:** Correo electrónico de socialización de información del Sistema de Gestión de Seguridad de la Información. **(A.6.3)**
Analizar, tramitar las solicitudes y realizar la colocación de recursos a los registros viables por concepto de Atención Humanitaria y Ayuda Humanitaria.	**Posibilidad de pérdida económica y reputacional por pérdida a la Integridad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el uso adecuado de la información.**	Muy baja	Moderado	Moderado	El líder del Proceso de Gestión para la Asistencia establece los perfiles de acceso a los funcionarios, contratistas y/o operadores de acuerdo con las actividades a desarrollar, a través del "Acuerdo de Confidencialidad" de cada uno de ellos, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión para la asistencia y/o reporte de dicho registro. **(A.6.6)**	**Moderado**	Reducir - Mitigación	**El Proceso de Gestión para la Asistencia define la herramienta SharePoint para el almacenamiento de la información del proceso, por lo que cada vez que se requiera un permisos específico de acceso se remitirá solicitud a la Oficina de Tecnología de Información (OTI)** **Evidencias: Correo de solicitud cada vez que se requiera el acceso. En caso de no tener solicitudes se deberá enviar correo por parte del líder del proceso indicando que en el periodo no se efectuó dicho requerimiento.** **[A.5.16, A.8.2, A.8.3, A.8.18]**

3.7. Riesgos de Gestión Prevención Urgente y Atención en la Inmediatez

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Ejecutar los controles que se generen como resultado del análisis, evaluación y calificación de los aspectos e impactos ambientales, los peligros que afecten la seguridad y la salud en el trabajo, los activos de seguridad de la información y los riesgos operativos y de corrupción	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables.	Alta	Mayor	Alto	El Proceso de Prevención Urgente y Atención en la Inmediatez suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas y/o operadores del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Proceso de Prevención Urgente y Atención en la Inmediatez y/o reporte de dicho registro. **(A.6.6)**	**Moderado**	Reducir - Mitigación	El Proceso de Prevención Urgente y Atención en la Inmediatez retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13)**
					El Proceso de Prevención Urgente y Atención en la Inmediatez no cuente con la disponibilidad de la información cuando está es eliminada por equivocación, se procederá a realizar reprocesos para la recuperación de la información de forma manual con el fin de tener toda la información disponible. **Evidencia:** Correos de gestión de la información que se esta recuperando. En el caso de que en el período no se allá efectuado recuperación de información, se deberá enviar correo indicándole al líder de proceso que no se efectuó dicho requerimiento. **(A.5.1, A.5.2, A.5.3, A.5.4, A.5.10, A.5.11)**			
					El Proceso de Prevención Urgente y Atención en la Inmediatez define la herramientas SharePoint para el almacenamiento de la información del proceso, por lo que cada vez que se requiera un permisos especifico de acceso se remitirá solicitud a la Oficina de Tecnología de Información (OTI). **Evidencia:** Correo de solicitud cada vez que se requiera el acceso. En caso de no tener solicitudes se deberá enviar correo por parte del líder del proceso indicando que en el periodo no se efectuó dicho requerimiento. **(A.5.16, A.8.2, A.8.3, A.8.13)**			

3.8. Riesgos de Relación con el Ciudadano

Tramitar y elaborar la respuesta a peticiones quejas, reclamos y consultas interpuestos por los ciudadanos, víctimas, entidades y organismos de control. Registrar las solicitudes e informar a la población víctima sobre los trámites y servicios de la Unidad, a través del canal presencial, con el fin de lograr el acceso a la oferta institucional de la población víctima. Registrar información y socializar los trámites, campañas y servicios de la Unidad a través del canal telefónico y virtual, con el fin de orientar y lograr el acceso de la población víctima a la información referente a sus procesos o información de la entidad Notificar las Actuaciones Administrativas emitidas por la entidad a los ciudadanos, víctimas, presentantes, apoderados o, a las personas debidamente autorizadas. Analizar la viabilidad, verificar el cumplimiento del procedimiento y realizar la gestión correspondiente para el desarrollo de las estrategias complementarias para la atención y orientación.	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	Alta	Mayor	Alto	El Proceso de Relación con el Ciudadano suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas y/o operadores del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Relación con el Ciudadano y/o reporte de dicho registro. **(A.6.6)**	**Alto**	Reducir - Mitigación	El Proceso de Relación con el Ciudadano reportará cualquier evento y/o incidente de Seguridad que se presente en el proceso y que afecte la confidencialidad de la información de las víctimas. **Evidencia:** Correos de notificación del evento y/o incidente de seguridad, en caso de que no se presente se genera un correo al líder del proceso indicando que en la vigencia no se presento eventos y/o incidentes de seguridad de la información. **(A.6.8)**
					El Proceso de Relación con el Ciudadano de acuerdo a las solicitudes generadas por sospecha de fuga de información, procede a realizar una actividad de auditoria para validar que usuarios del Sistema de Gestión de Victimas (SGV) están ingresando en horario no permitido, esta actividad se realiza por demanda. **Evidencia:** Correo de sospecha de fuga de información y/o correo de solicitud de eventos efectuados en el periodo. **(A.5.15, A.5.33, A.6.8)**			Las personas de Servicio al Ciudadano encargadas de los canales de atención generan notas informativas de sensibilización de los temas de seguridad y privacidad de la información a los usuarios de los diferentes canales de atención. **Evidencia:** notas informativa de sensibilización de los temas de seguridad. **(A.6.3)**
					El Proceso de Relación con el Ciudadano envia correo a la Subdirección de Asistencia y Atención Humanitaria solicitando reporte de usuarios inactivos del periodo a reportar (gestionado) de los Sistemas de Información relacionados al Proceso. **Evidencia:** Correo de solicitud del reporte de inactivación y respuesta de la Subdirección de Asistencia Humanitaria. **(A.5.15, A.5.16, A.5.17, A.5.18, 8.3, 8.26)**			El Proceso de de Relación con el Ciudadano asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen y el enlace SIG socializar la información del Sistema de Gestión de Seguridad de la Información a los funcionarios, contratistas y operadores del proceso cada vez que la Oficina de Tecnología de la Información (OTI) las publique. **Evidencia:** Correo electrónico replicados por el enlace del proceso para participar en las charlas de seguridad de la información, socialización de información del Sistema de Gestión de Seguridad de la Información y listas de asistencias a las charlas. **(A.6.3)**

3.9. Riesgos de Reparación Integral

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Transversal al Proceso Reparación Integral.	Posibilidad de pérdida económica y reputacional por divulgación o alteración no autorizada de los sistemas de información y/o la información sensible registrada en documento físico o digital a la que se tiene autorización de acceso (Activos críticos asociados), debido a vandalismo o hurto por ausencia o insuficiencia de controles de acceso al archivo digital, acciones involuntarias y/o deliberadas de usuario por ausencia o insuficiencia en la gestión de eventos de monitoreo o por almacenamiento de información sin protección, acceso no controlado a información sensible / confidencial, desconocimiento de los procedimientos y controles de Seguridad de la Información y/o por omisión o inadecuado proceso de identificación y calificación de los activos de información. *Activos críticos asociados.	Baja	Mayor	Alto	El Proceso Reparación Integral como administrador de las herramientas tecnológicas del Proceso a través de los profesionales designados, forman, capacitan y sensibilizan a los colaboradores para que hagan uso responsable en el acceso y manejo de la información del Proceso Reparación Integral cada vez que se realicen ajustes que afecten los procesos de las herramientas. **Evidencia:** contamos con soportes de las socializaciones y/o listados de asistencia. **(A.6.3).**	**Alto**	Reducir - Mitigación	El Proceso de Reparación Integral asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información, comunicación interna del material de seguridad generada por la Oficina de la Tecnologías de la Información (OTI) y listas de asistencia; replicadas por el enlace del proceso. **(A.6.3)**
					El Proceso de Reparación Integral suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas y/o colaboradores de los operadores de Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de NO contar con el "Acuerdo", no se asignará accesos ni usuarios, para el caso de que se venza el "Acuerdo" el usuario será deshabilitado. **Evidencia:** se cuenta con la relación mensual de usuarios de las herramientas y los acuerdos de confidencialidad suscritos. **(A.6.6)**			Implementar nuevas acciones de seguridad para el uso de los sistemas de información del Proceso Reparación Integral en articulación de la Oficina de Tecnologías de Información. **Evidencia:** tenemos correos electrónicos con los soportes de solicitudes y el trabajo realizado, sino se realiza tendremos un correo con el soporte de la no realización. **(A.8.26).**
					Los administradores de las herramientas tecnológicas del Proceso Reparación Integral cada vez, generan mensajes de confirmación y validación frente a las transacciones (insertar, actualizar o eliminar) de información sobre el sistema de información. En caso de no confirmar la acción la información no se actualizará. **Evidencia:** tenemos pantallazos de los sistemas de validación implementados en las herramientas y/o logs de auditoría. **(A.8.34)**			Atender a los requerimientos de la Oficina de Tecnologías de la información frente a los planes de mejoramiento de seguridad de la información cuando sea requerido el proceso. **Evidencia:** tenemos os correos electrónicos con las solicitudes, sino se realiza tendremos un correo con el soporte de la no realización. **(A.8.26, A.5.35, A.5.36).**

3.10. Riesgos de Comunicación Estratégica

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Implementar la estrategia de comunicación política para la dignificación de las víctimas del conflicto armado y la construcción de la paz	**Posibilidad de pérdida económica y reputacional ante nuestras partes interesadas, por quejas o sanciones ocasionadas por comunicación interna y/o externa inadecuada, generando una pérdida de la integridad de la información de la Entidad, debido a la falta o ausencia de controles relacionados con el uso adecuado de la misma.**	Media	Moderado	Moderado	El grupo de comunicación digital de la Oficina Asesora de Comunicaciones, tiene establecido un código de verificación en dos pasos que se activa cada vez que alguno de los funcionarios autorizados con contraseña acceden desde otro dispositivo a cualquiera de las redes sociales de la Unidad. Los códigos solo serán recibidos por el funcionario de planta que hace parte del equipo digital. En el caso de las transmisiones con otras entidades o usuarios externos, no se comparten las contraseñas de las redes, se realiza por transmisión cruzada y envío de rtmp (protocolo de mensajería en tiempo real) por parte de la Unidad. **Evidencia:** Correo por parte del líder de comunicación digital que indique que se presento o no solicitudes en el periodo. **(A.8.5, A.8.24)**	**Moderado**	Reducir - Mtigación	El Proceso de Comunicación Estratégica asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información, comunicación interna del material de seguridad generada por la Oficina de la Tecnologías de la Información (OTI) y listas de asistencia; replicadas por el enlace del proceso. **(A.6.3)**

3.11. Riesgos de Direccionamiento Estratégico

Implementar las estrategias establecidas por el Sistema de Seguridad de la Información a interior del proceso	Posibilidad de pérdida reputacional de la entidad por la divulgación o alteración no autorizada de los activos de información, debido a ausencia o insuficiencia de copias de respaldo, falta de apropiación de las políticas de privacidad de la información y ausencia o insuficiencia de documentación de uso y/o administración.	Media	Leve	Moderado	El profesional de la OAP, se encarga de revisar e inactivar los usuarios, cuando se retiran de la Unidad, o cambian de proceso en la herramienta utilizada por la OAP, en los módulos Plan de Acción y SIG. Esta actualización se realiza mediante correo electrónico. En caso de que no se solicite una revisión, la misma se realizara de manera trimestral para mantener la herramienta actualizada. **Evidencia:** Correos electrónicos de solicitud y/o correo electrónico de la revisión trimestral de la herramienta del proceso. **(A.5.15, A.5.16, A.5.18)**	**Bajo**	Aceptar	N/A
					El Proceso de Direccionamiento Estratégico define las herramientas SharePoint para el almacenamiento de la información del proceso, por lo que cada vez que se requiera un permisos específico de acceso se remitirá solicitud a la Oficina de Tecnología de Información (OTI). **Evidencia:** Correo de solicitud cada vez que se requiera el acceso. En caso de no tener solicitudes, se deberá enviar correo por parte del líder del proceso indicando que en el periodo no se efectuó dicho requerimiento. **(A.5.16, A.8.2, A.8.3, A.8.13)**			
					El Proceso de Direccionamiento Estratégico asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información, comunicación interna del material de seguridad generada por la Oficina de la Tecnologías de la Información (OTI) y listas de asistencia; replicadas por el enlace del proceso. **(A.6.3)**			

3.12. Riesgos de Gestión Administrativa

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Controlar y hacer seguimiento a la atención de los servicios generales necesarios para el buen funcionamiento de la entidad (papelería, vigilancia, seguros, transporte, aseo y cafetería mantenimiento)	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falta de controles de acceso físico y perimetrales de las instalaciones de la UARIV, por ingreso de personal no autorizado.	Media	Mayor	Alto	El Proceso de Gestión Administrativa realiza la contratación de Vigilancia, con el fin preservar la seguridad de los activos de información y los Colaboradores de la Entidad. **Evidencia:** Contrato de Vigilancia de la Vigencia. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11)** El Proceso de Gestión Administrativa, define como mecanismo de control para el acceso de personal a las instalaciones de la Entidad, el registro en la herramienta "Ingreso San Cayetano Power App" por parte de las áreas que requieran la autorización de ingreso. **Evidencia:** Registro en la herramienta y/o informe y/o correo de generación de la solicitud de las áreas que requieran autorización de ingreso. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11)**	**Alto**	Reducir - Mitigación	El Proceso de Gestión Administrativa, realiza el seguimiento mensual al Proveedor de Vigilancia con fin de verificar el cumplimiento de las actividades enmarcadas en el Contrato. **Evidencia:** Informe de ejecución del contrato de vigilancia. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11)**
Controlar y hacer seguimiento a la atención de los servicios generales necesarios para el buen funcionamiento de la entidad (papelería, vigilancia, seguros, transporte, aseo y cafetería mantenimiento)	Posibilidad de pérdida de disponibilidad y/o continuidad del Servicio eléctrico, debido a falta o ausencia de mantenimiento preventivo de la planta eléctrica y ups del complejo empresarial San cayentano donde opera la Entidad.	Baja	Moderado	Moderado	El Proceso de Gestión Administrativa, realiza el seguimiento a la Administración del Complejo San Cayetano donde opera la Entidad, frente al cumplimiento de las pruebas y mantenimiento de la (PLANTA ELÉCTRICA) de manera bimensual con el objetivo de garantizar la Continuidad del Servicio y tomar medidas correctivas. **Evidencia:** Envío del correo electrónico bimensual del Proceso de Gestión Administrativa a la Administración del Complejo para el seguimiento de las pruebas y mantenimiento y cronograma de mantenimientos (PLANTA ELÉCTRICA) y informes de (pruebas y mantenimiento) de la PLANTA ELÉCTRICA ejecutadas por la Administración del Complejo. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11)** El Proceso de Gestión Administrativa, realiza el seguimiento a la Administración del Complejo San Cayetano donde opera la Entidad, frente al cumplimiento de las pruebas y mantenimiento de la (UPS) de manera bimensual con el objetivo de garantizar la Continuidad del Servicio y tomar medidas correctivas. **Evidencia:** Envío del correo electrónico bimensual del Proceso de Gestión Administrativa a la Administración del Complejo para el seguimiento de las pruebas y mantenimiento y cronograma de mantenimientos (UPS) y informes de (pruebas y mantenimiento) a la UPS ejecutadas por la Administración del Complejo. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11)** El Proceso de Gestión Administrativa, en caso de identificar que no se están realizando las actividades de (pruebas y mantenimientos) preventivos para la (PLAN Y ELÉCTRICA Y UPS) donde opera la Entidad y/o se presentó una indisponibilidad en la continuidad del servicio eléctrico, se procederá a realizar un comunicado a la Administración del Complejo San Cayetano frente a las fallas o ausencias de los mantenimientos afectaron los servicios que presta la UARIV. **Evidencia:** Correo electrónico del Proceso de Gestión Administrativa por el incumplimiento de las (pruebas y mantenimientos) preventivos de la (PLAN Y ELÉCTRICA Y UPS) y/o en caso de que no se materialice el riesgo el líder del proceso envía correo al Oficial de Seguridad de la Información de la Entidad indicando que para el presente periodo no se presentó indisponibilidad del servicio eléctrico en las instalaciones de la entidad del nivel nacional. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11)**	**Bajo**	Aceptar	N/A

3.13. Riesgos de Gestión de la Información

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Gestionar la capacidad de los recursos y servicios TI, con el fin de controlar y racionalizar la oferta y el rendimiento de la infraestructura informática. Gestionar la infraestructura tecnológica asociada a los servicios de: buzones de correo institucional, acceso a servidores y bases de datos (solo aplica a desarrolladores),telefonía IP.	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables para la implementación de políticas de backups, gestión de identidades, control de acceso a los recursos y/o repositorios de la información.	Alta	Catastrófico	Extremo	El proceso de Gestión de la Información, en cabeza de Dominio de Infraestructura TI, realiza ejecución de los backups de acuerdo a la periodicidad establecidas para las bases de datos. **Evidencia:** Reporte donde se observa los backups y/o logs de ejecución del backup de las bases de datos realizadas en el periodo por el del Dominio de Infraestructura TI. **(A.8.13)**	**Extremo**	Reducir - Mitigación	El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI, realizará pruebas de restauración Backup. **Evidencia:** Reporte donde se observa la restauración de backups ejecutados en el periodo el Dominio de Infraestructura TI. **(A.8.13)**
					El proceso de Gestión de la Información, en cabeza de Dominio de Infraestructura TI realiza ejecución de los backups de acuerdo a la periodicidad establecida para la configuración de servidores, dispositivos de red. **Evidencia:** Reporte donde se observa los backups ejecutados en el periodo por el del Dominio de Infraestructura TI. **(A.8.13)**			El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI, atiende los casos reportados en la herramienta de gestión "ARANDA" para la creación o inactivación de de usuarios (Funcionario, contratista o operador) de la Entidad. **Evidencia:** Registro de los casos reportados y atendidos en la herramienta de gestión "ARANDA" por Dominio de Infraestructura TI. **(A.5.15, A.5.16, A.5.17, A.5.18, 8.3, 8.26)**
					El proceso de Gestión de la Información, en cabeza de Dominio de Infraestructura TI, aplica controles de acceso a los usuarios de cada proceso para (consulta, adición y modificación) de la información en la herramienta de SharePoint de la Entidad. **Evidencia:** Correo de solicitud de los procesos para conceder los permisos asociados al repositorio de SharePoint en el periodo y/o correo del líder del Dominio que indique que para el presente periodo no se recibieron solicitudes de accesos. **(A.5.2, A.5.3, A.5.15)**			El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI, realiza la gestión y seguimiento del mantenimiento preventivo de las UPS y/o dispositivo de red del Nivel Territorial de la Entidad ejecutado por el operador. **Evidencia:** Programación y seguimiento del mantenimiento preventivo y correctivo y/o correo del líder del dominio que indique que para el presente periodo no se realizo mantenimiento preventivo y correctivo. **(A.5.15, A.5.16, A.8.2)**
Desarrollar nuevas aplicaciones y sistemas de información. Soportar sistemas de información y aplicaciones.	Posibilidad de pérdida económica y reputacional por pérdida a la Integridad y disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables para el acceso a los recursos, uso adecuado de la información y la ejecución del control de cambios de (nuevos desarrollos y/o actualizaciones).	Media	Mayor	Alto	El proceso de Gestión de la Información, en cabeza de Dominio de Sistemas de Información, registran los backlogs en Azure Devops con el fin de llevar un control de los nuevos desarrollos y/o actualizaciones de los sistemas de información que fueron aceptados y aprobados. **Evidencia:** Pantallazo del registro de los backlogs en Azure Devops afectados en el periodo y/o correo del líder de Dominio que indique que para el presente periodo no se realizaron desarrollos nuevos o actualizaciones. **(A.8.14)**	**Alto**	Reducir - Mitigación	El Proceso de Gestión de la Información desde el dominio de Sistemas de Información, deberá realizar la sincronización con OneDrive de la información que se procese o almacene en los equipos de cada uno de los colaboradores al interior del dominio de Sistemas de Información. **Evidencia:** Pantallazo de sincronización en OneDrive de los equipos de los colaboradores del Dominio de Sistemas de Información y/o la acción a tomar para los casos que no cumplen con la sincronización y uso de OneDrive. **(A.5.16, A.8.2, A.8.3, A.8.13)**
					El proceso de Gestión de la Información, en cabeza de Dominio de Sistemas de Información, realiza la verificación de controles aplicables que son requisitos de seguridad en el ciclo de vida de desarrollo de software para los nuevos desarrollos y/o actualizaciones. **Evidencia:** Archivo de verificación de los controles de seguridad y/o Pantallazo del archivo del registro de verificación de los controles de seguridad en Azure Devops y/o correo del líder del Dominio que indique que para el presente periodo no se realizaron desarrollos nuevos o actualizaciones. **(A.8.25, A.8.26)**			El Proceso de Gestión de la Información desde el dominio de Sistemas de Información, asistirá y participará en las capacitaciones del Sistema de Gestión de Seguridad de la Información SGSI, brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen. **Evidencia:** Lista de asistencia de las charlas de seguridad de la información donde se evidencia la participación de los Colaboradores del Dominio de Sistemas de Información. **(A.6.3)**
					El proceso de Gestión de la Información, en cabeza de Dominio de Sistemas de Información, implementa el protocolo de gestión de control de cambios para los desarrollos nuevos y/o actualizaciones de los sistema de información. **Evidencia:** Registro de formato de cambios y/o acta de comité de control de cambios aprobados y/o rechazados y/o correo del líder del Dominio que indique que para el presente periodo no se presentaron controles de cambios por desarrollos nuevos o actualizaciones. **(A.8.32)**			

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Dotar tecnológicamente en casos de traslado de sede, nueva sede o adicionales, así como realizar la validación de infraestructura e inventario tecnológico en las sedes.	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	Alta	Mayor	Alto	El proceso de Gestión de la Información, en cabeza de Dominio de Servicios TI, suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas Y/o Operadores del Proceso cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado . Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el Dominio de Servicios TI y/o correo del líder del dominio que indique que para el presente periodo no se suscribieron Acuerdos de Confidencialidad. **(A.6.6)** El proceso de Gestión de la Información, en cabeza de Dominio de Servicios TI, realiza la segregación de tareas en la atención o ejecución del soporte técnico solicitado a través de la Mesa de Servicios Tecnológicos. **Evidencia:** Segregación de tareas en la herramienta de gestión "ARANDA". **(A 5.2, A.5.3, A.5.4)** El proceso de Gestión de la Información, en cabeza de Dominio de Servicios TI, realiza reporte en la herramienta de gestión "ARANDA" para la creación o inactivación de de usuarios (Funcionario, contratista o operador) del Dominio Servicios TI. **Evidencia:** Registro de los casos reportados para la creación o inactivación de usuario en la herramienta de gestión "ARANDA". **(A.5.15, A.5.16, A.5.17, A.5.18, 8.3, 8.26)**	**Alto**	Reducir - Mitigación	El Proceso de Gestión de la Información desde el Dominio de Servicios TI, asistirá y participará en las capacitaciones del Sistema de Gestión de Seguridad de la Información SGSI, brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen. **Evidencia:** Lista de asistencia de las charlas de seguridad de la información donde se evidencia la participación de los Colaboradores del Dominio de Sistemas de Información. **(A.6.3)**
Formular políticas, planes, estrategias y/o proyectos, adoptando lineamientos y estándares según corresponda.	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables que permiten dar cumplimiento a las políticas y lineamientos relacionados con los principios de Arquitectura Empresarial.	Media	Moderado	Moderado	El proceso de Gestión de la Información, en cabeza de Dominio de Arquitectura Empresarial, realiza la revisión, actualización y seguimiento del Plan Estratégico de Tecnología de la Información (PETI) con el fin de que este integre y cumplan con los proyectos definidos en el Plan Estratégico de Seguridad de la Información (PESI) de acuerdo a los lineamientos del Gobierno Nacional. **Evidencia:** Acta de las mesas de trabajo para la actualización del PETI y/o acta de seguimiento del PETI. **(A 5.1, A.5.2, A.5.8, A.5.36)** El proceso de Gestión de la Información, en cabeza de Dominio de Arquitectura Empresarial, realiza la revisión y/o actualización del documento Marco de Referencia de Arquitectura Empresarial de la Entidad de acuerdo a los lineamentos de MinTIC. **Evidencia:** Acta de las mesas de trabajo para la revisión y/o actualización del documento del Marco de Referencia de Arquitectura Empresarial y/o correo del líder del dominio que indique que para el presente periodo no se realizo revisión y/o actualización del documento. **(A.5.36)**	**Moderado**	Reducir - Mitigación	El Proceso de Gestión de la Información desde el Dominio de Arquitectura Empresarial, deberá realizar la sincronización con OneDrive de la información que se procese o almacene en los equipos de cada uno de los colaboradores al interior del Dominio de Arquitectura Empresarial, **Evidencia:** Pantallazo de sincronización en OneDrive de los equipos de los colaboradores del Dominio de Arquitectura Empresarial y/o la acción a tomar para los casos que no cumplen con la sincronización y uso de OneDrive. **(A.5.16, A.8.2, A.8.3, A.8.13)** El Proceso de Gestión de la Información desde el Dominio de Arquitectura Empresarial, asistirá y participará en las capacitaciones del Sistema de Gestión de Seguridad de la Información SGSI, brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen. **Evidencia:** Lista de asistencia de las charlas de seguridad de la información donde se evidencia la participación de los Colaboradores del Dominio de Sistemas de Información. **(A.6.3)**

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Identificar los riesgos, aplicar los controles e implementar el plan de respuesta a los riesgos. Gestionar las actividades derivadas de la implementación del subsistema de gestión de seguridad de la información.	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la fallas en la identificación y seguimiento de los riesgos de Seguridad y desactualización del Inventario de Activos de Información de la Entidad.	Alta	Mayor	Alto	El proceso de Gestión de la Información, en cabeza de Dominio de Seguridad, realiza seguimiento y gestión con cada uno de los Procesos del Nivel Central y Dirección Territorial la actualización periódica del Inventario de Activos de Información de la Entidad. **Evidencia:** Correo de programación de mesas de trabajo para actualización del Inventario y/o Inventario de Activos actualizados de los Procesos y Direcciones Territoriales. **(A.5.9)**	**Alto**	Reducir - Mitigación	El proceso de Gestión de la Información, en cabeza del Dominio de Seguridad, realiza seguimiento y gestión para aumentar el porcentaje de cumplimiento del Instrumento del Modelo de Seguridad y Privacidad de la Información (MSPI). **Evidencia:** Instrumento del Modelo de Seguridad y Privacidad de la Información (MSPI). **(A.5.36)**
					El proceso de Gestión de la Información, en cabeza de Dominio de Seguridad, realiza la presentación para aprobación de los Activos de Información y los Instrumentos de Gestión Pública ante el Comité de Gestión y Desempeño Institucional de la Entidad. **Evidencia:** Presentación de los Activos de Información a Comité de Gestión y Desempeño Institucional y/o acta de aprobación de los Instrumentos de Gestión de Información Pública. **(A.5.9)**			El proceso de Gestión de la Información, en cabeza del Dominio de Seguridad, definirá un Plan de Cultura y Sensibilización en Seguridad de la Información y realizará seguimiento de las actividades definidas. **Evidencia:** Plan de Cultura aprobado y/o seguimiento de las actividades definidas y desarrolladas mensualmente. **(A.6.3)**
					El proceso de Gestión de la Información, en cabeza del Dominio de Seguridad, realiza seguimiento y actualización de los Riesgos de Seguridad de la Información con cada uno de los Proceso y Direcciones Territoriales de la Entidad. **Evidencia:** Informe de seguimiento de los Riesgos de Seguridad de la Información y/o matriz de riesgos actualizada. **(A.5.35, A.5.36)**			
Identificar los riesgos, aplicar los controles e implementar el plan de respuesta a los riesgos.	Posibilidad de pérdida económica y reputacional por pérdida a la Integridad y Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles para la remediación de vulnerabilidades en la Infraestructura Tecnológica y/o materialización de incidentes de seguridad.	Alta	Catastrófico	Extremo	El proceso de Gestión de la Información, en cabeza de Dominio de Seguridad, realiza semestral análisis de vulnerabilidades a la Infraestructura Tecnológica (Sistemas de Información y Servicios TI) de la Entidad. **Evidencia:** Reporte de análisis de vulnerabilidades a la Infraestructura Tecnológica (Sistemas de Información y Servicios TI) semestral. **(A.8.8)**	**Alto**		El proceso de Gestión de la Información, en cabeza del Dominio de Seguridad, realizara revisión de la configuración de las herramientas de seguridad con el fin de verificar la aplicación de la Política de restricción para el uso de medios de almacenamiento de información (USB) implementada en la Entidad. **Evidencia:** Pantallazos de la configuración de la política de restricción para el uso de medios de almacenamiento de información (USB) a cinco (5) usuarios por proceso aleatorios de forma mensual. **(A.8.9)**
					El proceso de Gestión de la Información, en cabeza de Dominio de Seguridad, realizara mesas de trabajo con los responsables de cada Servicios TI con el fin de establecer las actividades, fechas y responsables de las remediaciones de las vulnerabilidades identificadas en la Infraestructura Tecnológica de la Entidad. **Evidencia:** Seguimiento al Plan de remediaciones de vulnerabilidades identificadas en el mes. **(A.8.8, A.8.12)**			El proceso de Gestión de la Información, en cabeza del Dominio de Seguridad, verificación que los equipos de propiedad de la Entidad tenga instalado y actualizado el agende de antivirus. **Evidencia:** Registro mensual de la consola de los equipos que se sincroniza. **(A.8.20, A.8.21)**
					El proceso de Gestión de la Información, en cabeza del Dominio de Seguridad, en el marco del cumplimiento de Procedimiento de Incidentes de Seguridad realizará la gestión a los incidentes reportados en la herramienta de gestión "ARANDA" los cuales deberán estar documentados como base de conocimiento, con lo cuales permitan dar solución a futuros eventos de seguridad. **Evidencia:** Reportes de casos mensuales en aranda. **(A.5.24, A.5.25, A.5.26, A.5.27, A.5.28)**			

Proceso / Dirección Territorial / Dueño del Riesgo	Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Gestión de la Información	Alistar y disponer las fuentes y bases de datos de información de la población víctima de acuerdo con la necesidad, en las herramientas aplicativos y visores utilizados por la SRNI.	Posibilidad de pérdida reputacional por la indisponibilidad de fuentes, bases de datos de información y/o sistemas de información de la población víctima de acuerdo con la necesidad, en las herramientas, aplicativos y visores utilizados por la SRNI, debido a que las entidades limitan el intercambio de información bajo argumentos políticos legales o voluntades personales, la falta de infraestructura tecnológica adecuada y disponible, e incumplimiento por parte de las entidades externas receptoras de la información, de los acuerdos y/o convenios de intercambio de información firmados con la Unidad, o porque la información de los sistemas de información internos tienen deficiencias en la calidad de los datos que se generan y que se utiliza como insumo para la gestión.	Baja	Menor	Moderado	El procedimiento de Articulación interinstitucional y dinamización de la información AIDI, realiza por demanda la oficialización del acuerdo de intercambio de información, generando un anexo técnico al anterior documento donde se encuentran las reglas que rigen el intercambio, acompañado del diccionario de datos, que es el insumo para el entendimiento de la fuente; para las entidades que no aplican documento técnico esta información queda en un oficio, correo electrónico o acta. De igual manera se realiza un seguimiento a lo estipulado en el documento técnico a través del oficio, correos electrónicos o actas de reunión. **Evidencia:** Anexo técnico, oficio, correo electrónico o acta. En caso de que la solicitud no tenga acuerdo o esté incompleta, no se realizara el cargue de información a los sistemas de la SRNI. **(A.5.14)** La Subdirección Red Nacional de Información-SRNI, cada vez que se requiera, solicita a través de correo electrónico o acta de reunión a la Oficina de Tecnologías de Información o al personal encargado de la actividad la ampliación del recurso tecnológico, con el fin de soportar las nuevas necesidades en el intercambio de información. En caso de no recibir respuesta por parte del personal encargado se programa reunión con los jefes de las áreas técnicas para definir los alcances y motivos de la demora en la respuesta. **Evidencia:** Correo electrónico o Acta de reunión. **(A.8.6)** El Procedimiento de Articulación interinstitucional y dinamización de la información-AIDI, cada vez que se realiza el corte de las fuentes verifica el cumplimiento de lo establecido en los acuerdos y/o convenios entre la Unidad y las Entidades Nacionales, a través de los cortes dispuestos en la herramienta Vivanto contra lo establecido en los acuerdos de intercambio, con el objetivo de garantizar información actualizada que dé cuenta de los datos asociados a la población víctima. En caso de incumplimiento, se notifica a la entidad respectiva. **Evidencia:** Como evidencia de lo anterior se encuentra el envío del correo electrónico, acta u oficio. **(A.5.14)** El profesional de Gestión de la Información (AIDI), cada vez que reciba una fuente realiza una validación de la misma en particular para las mediciones de Subsistencia Mínima, Superación de Situación de Vulnerabilidad e Indicadores de Goce Efectivo de Derechos, de acuerdo a las variables mínimas requeridas con el fin de validar la consistencia de variables a intercambiar con la entidad o área misional que se tiene el intercambio. En caso de inconsistencias se devuelve la fuente solicitando aclaraciones. **Evidencia:** El soporte de este control es la aprobación de metadato en el inventario de fuentes. Correo electrónico o el cargue en Vivanto. **(A.5.14)**	**Bajo**	Aceptar	N/A
Gestión de la Información	Levantamiento de información a través de entrevista de caracterización.	Posibilidad de pérdida reputacional por divulgación o alteración no autorizada de información, con ocasión a la perdida o hurto de la misma, debido al extravío o hurto del dispositivo en campo o herramientas donde se está tomando la encuesta en el esquema de acompañamiento presencial del levantamiento de información a través de entrevista de caracterización.	Media	Leve	Moderado	El equipo SRNI a demanda realiza configuración de dispositivos que son propiedad de la Subdirección Red Nacional de Información con bloqueo por contraseña. Una contraseña para que el dispositivo salga del modo de suspensión en el que ingresa, tras un período de inactividad. Medida que se complementa con el cifrado de la memoria y dicha clave solo está en poder de la SRNI. **Evidencia:** Se evidencia con las tablets utilizadas en los levantamientos de información las cuales se encuentran bajo custodia de la Subdirección. **(A.5.3, A.5.16, A.8.2)** El equipo SRNI a demanda articula la implementación de la caracterización con las mesas de víctimas y demás actores del territorio. **Evidencia:** como evidencia se tiene actas de reuniones, convenios interinstitucionales, oficios o correos electrónicos. En caso de no contar con la solicitud no se podrá atender esta clase de requerimiento. **(A.6.3)** El equipo SRNI socializa y capacita el manejo de herramientas tecnológicas y aplicativo al personal que realiza el levantamiento de información (presencial y no presencial), cada vez que la entidad solicita acompañamiento. **Evidencia:** como evidencia se tiene actas de reunión, listas de asistencia , oficios o correos electrónicos de la capacitación. En caso de no ser viable su ejecución, no se podrá activar usuarios para el levantamiento de información. **(A.6.3)** La mesa de servicio, inactiva los usuarios del modulo de caracterización (versión WEB y OFFLINE)de la siguiente forma 1. los usuarios se inactivan de acuerdo a su periodo de vinculación contractual. 2. El primero de enero de cada vigencia se inactivan todos los accesos a Vivanto. 3. Bloqueo automático por no registrar actividad del usuario en un periodo de 30 días calendario. 4. A solicitud de las entidades externas o cliente interno. En caso de detectar mal uso de la herramienta se inactivará el usuario. **Evidencia:** Estado inactivo en la herramienta Vivanto. Con el objetivo de asegurar que las personas que consultan la información de la población víctima son funcionarios y servidores públicos que en el marco de sus funciones necesitan acceder a esta información. **(A.5.3, A.5.16, A.8.2, A.5.17, A.5.18)**	**Moderado**	Reducir - Mitigación	La Subdirección Red Nacional de Información (SRNI), asistirá y participará en las capacitaciones del Sistema de Gestión de Seguridad de la Información SGSI, brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen. **Evidencia:** Lista de asistencia de las charlas de seguridad de la información donde se evidencia la participación de los Colaboradores de la Subdirección Red Nacional de Información (SRNI). **(A.6.3)**

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
* Dar trámite a las solicitudes de información realizadas por el cliente interno o entidades externas.	Posibilidad de pérdida reputacional por captura y/o uso inadecuado de la información de identificación personal recopilada sobre los datos de la población víctima por parte de encuestador de la UARIV, debido a la falta de control en el dispositivo móvil off-line traería como consecuencia usar la Identificación Personal con propósitos desconocidos o ilegales.	Media	Mayor	Alto	Cada vez que se contrata a un colaborador el Subdirector de la Red Nacional de Información condiciona a los colaboradores encargados del procesamiento de Identificación Personal a ejecutar sus actividades previa a la suscripción de un acuerdo de confidencialidad que garantice el compromiso ético de utilizar la información en debida forma. En caso de no de no firmar el acuerdo de confidencialidad no se podrá procesar Información. **Evidencia:** queda el acuerdo de confidencialidad firmado del Colaborador. **(A.6.6)** Controles de transmisión donde se incluya Identificación Personal: Cada vez que se requiera el líder de Estrategia de Caracterización implementa la trazabilidad en la transmisión de IIP garantizando el encriptamiento de la información para su disposición en el servidor. En caso de no implementar la trazabilidad en la transmisión de IIP no garantiza el encriptamiento de la información para su disposición en el servidor. **Evidencia:** queda el registro en el log del servidor. **(A.8.15)**	Bajo	Aceptar	N/A
Alistar y disponer las fuentes y bases de datos de información de la población víctima de acuerdo con la necesidad, en las herramientas, aplicativos y visores utilizados por la SRNI	Posibilidad de pérdida de confidencialidad por el uso indebido de la información dispuesta por la SRNI, ocasionado por un alto nivel de consultas en el aplicativo de VIVANTO para el modulo de consulta individual.	Alta	Leve	Moderado	El proceso de Gestión de la Información, en cabeza de la Subdirección Red Nacional de Información (SRNI), genera mensualmente auditorias internas a las consultas realizadas en el Portal VIVANTO. **Evidencia:** Registro de la auditoria mensuales al Portal VIVANTO. **(A.5.15, A.5.33, A.8.34)** El proceso de Gestión de la Información, en cabeza de la Subdirección Red Nacional de Información (SRNI), brinda socializaciones sobre el uso adecuado del Portal VIVANTO. **Evidencia:** Socialización del uso adecuado y/o lista de asistencia. **(A.6.3)** El proceso de Gestión de la Información, en cabeza de la Subdirección Red Nacional de Información (SRNI), inactiva usuario cuando se evidencien consultas elevadas en el mes inmediatamente anterior. **Evidencias:** Reporte de inactivación de usuarios por consultas elevadas en el mes. **(A.5.15, A.5.16, A.5.17, A.5.18, 8.3, 8.26)**	Bajo	Aceptar	N/A

3.14. Riesgos de Gestión Documental

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Proporcionar el servicio de préstamos y consulta de expedientes, que se encuentren bajo la administración del Archivo de la Entidad.	**Posibilidad de pérdida económica y reputacional por pérdida de la Integridad y Disponibilidad de la Información de la Entidad, debido a la falta o ausencia de controles de seguridad relacionados con el uso adecuado de los expedientes físicos que se encuentran almacenados en los archivos de gestión y central.**	Alta	Catastrófico	Extremo	El Proceso de Gestión Documental, realiza a través de la "Digitalización con fines probatorios" de los expedientes (con todos sus folios) el cargue de estas imágenes en el Sistema de Gestión de Documentos Electrónicos de Archivo "ARCHIDU" para garantizar y facilitar el acceso a la información y evitar la consulta de documentos físicos originales. **Evidencia:** Pantallazo de consulta de los expedientes digitalizados en ARCHIDU para el periodo y/o archivo de numero de expedientes digitalizados en el mes. **(A.5.13, A.5.15, A.8.15)** El Proceso de Gestión Documental, genera un inventario documental por dependencia y direcciones territoriales para llevar el registro de los expedientes que se encuentra en el archivo de gestión y central de la Entidad. **Evidencia:** Archivo de Excel del inventario documental por dependencia y direcciones territoriales. **(A.5.10, A.5.12, A.5.13, A.5.15, A.8.15)** El Proceso de Gestión Documental, cuando se genera una denuncia por pérdidas de un documento o expediente o cuando se identifica que los expedientes no están completos o les falte documentos originales, se aplica el procedimiento para la reconstrucción de expedientes y/o documentos. **Evidencia:** Informe de pérdida de documento y/o correo de notificación del líder del proceso indicando que no se presento novedades de perdida de documentos de otras dependencias en el periodo. **(A.5.33, A.8.15)**	Alto	Reducir - Mitigación	El Proceso de Gestión Documental, lleva el registro y control de prestamos de expedientes a los funcionarios y/o contratistas de la Entidad para la atención y trámites en sus dependencias del nivel nacional. **Evidencia:** Formato Préstamo de Documentos y/o Expedientes de Archivos de Gestión mensual. **(A.5.10, A.5.12, A.5.13, A.5.15, A.8.15)** El Proceso de Gestión Documental, cuenta con las tablas de control de acceso que permite clasificar la información de acuerdo a los lineamientos de Ley 1712 de 2014 (Información Pública Reservada, Información Pública Clasificada, Pública) parara los prestamos de los expedientes. **Evidencia:** Tablas de control de acceso y/o correos de respuesta de solicitudes de prestamos. **(A.5.10, A.5.12, A.5.13)**

3.15. Riesgos de Evaluación Independiente

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Identificar, analizar y priorizar los riesgos institucionales. (seguridad de la información).	**Posibilidad de pérdida reputacional de la información que gestiona la Oficina de Control Interno, debido al incumplimiento de las políticas de seguridad de la información, por no disponer de los datos en los repositorios asignando, desconocimiento de las herramientas y controles tecnológicos para el almacenamiento de la información gestionada por la Oficina de Control Interno, lo anterior se presenta por el desconocimiento de los lineamientos y políticas de seguridad del proceso de la OCI.**	Baja	Menor	Moderado	El profesional en Ingeniería de Sistemas de la OCI será el responsable de realizar capacitaciones y sensibilizaciones de políticas SGSI, desconocimiento de las herramientas y controles de seguridad de la información con una periodicidad semestral donde se darán a conocer los lineamientos de la seguridad de la información de la OCI, en caso de no realizarse en la fecha establecida se reprograma. **Evidencia:** se dejara la lista de asistencia y el correo de citación con sus anexos (memoria técnica). **(A.6.3)**	**Bajo**	Aceptar	N/A
Identificar, analizar y priorizar los riesgos institucionales. (seguridad de la información).	**Posibilidad de pérdida reputacional por la divulgación no autorizada de información que gestiona la Oficina de Control Interno, debido al no cumplimiento de las normas de auditorías generalmente aceptadas de la prudencia y reserva de la información y la generación de conflictos de intereses por parte de los auditores de la OCI,lo anterior por la falta de ética de los auditores.**	Baja	Menor	Moderado	El Proceso de Evaluación Independiente suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas del Proceso, cuando se requiere acceder al archivo físico y herramientas colaborativas como (OneDrive y SharePoint) en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado . **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión Contractual y/o reporte de dicho registro. **(A.6.6)**	**Bajo**	Aceptar	N/A

3.16. Riesgos de Gestión Interinstitucional

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Uso adecuado de los activos de información generados dentro de la Dirección de Gestión Interinstitucional	Posibilidad de pérdida reputacional ante nuestras partes interesadas por falta de disponibilidad y mal uso de los activos de información críticos del proceso,debido a la falta de apropiación de las políticas y lineamientos de Seguridad de la Información.	Media	Moderado	Moderado	El Proceso de Gestión Interinstitucional retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13)**	**Moderado**	Reducir - Mitigación	El Proceso de Gestión Interinstitucional asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información, comunicación interna del material de seguridad generada por la Oficina de la Tecnologías de la Información (OTI) y listas de asistencia. **(A.6.3)**
					El Proceso de Gestión Interinstitucional define la herramienta SharePoint para el almacenamiento de la información del proceso, por lo que cada vez que se requiera un permisos especifico de acceso se remitirá solicitud a la Oficina de Tecnología de Información (OTI) **Evidencia:** Correo de solicitud cada vez que se requiera el acceso. En caso de no tener solicitudes se deberá enviar correo por parte del líder del proceso indicando que en el periodo no se efectuó dicho requerimiento. **(A.5.16, A.8.2, A.8.3, A.8.13)**			

3.17. Riesgos de Participación y visibilización

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Actividades propias del proceso	Posibilidad de pérdida económica y reputacional ante las partes interesadas por divulgación o alteración no autorizada de la información y disponibilidad de la misma, debido a la ausencia o insuficiencia de procedimientos para la protección y acceso no controlado de la información sensible y/o confidencial.	Baja	Moderado	Moderado	El Proceso de Gestión Contractual retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. Evidencia: Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13)**	**Moderado**	Reducir - Mitigación	El Proceso de Participación y Visibilización, asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información y/o replicación del correo de comunicación interna en material de seguridad generada por la Oficina de la Tecnologías de la Información (OTI) y/o listas de asistencia. **(A.6.3)**
					El Proceso de Participación y Visibilización suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas del Proceso cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el "Acuerdo", no se asignara accesos ni usuarios; para el caso de que se venza el "Acuerdo" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarle a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Proceso de Participación y Visibilización y/o reporte de dicho registro. **(A.6.6)**			
					El Proceso de Participación y Visibilización aplica control de acceso a los usuarios para (consulta, adición y modificación) de la información en la herramienta de SharePoint. **Evidencia:** Correo de solicitud a la OTI y/o auxiliar del técnico del proceso para conocer los permisos asociados al SharePoint del Proceso. **(A.5.2, A.5.3, A.5.15)**			

3.18. Riesgos de Registro y Valoración

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Distribuir los formatos Únicos de Declaración -FUD- ó suministro de la herramienta de toma en línea a las oficinas del Ministerio Público para la recepción de la declaración junto a la documentación anexa.-Analizar, valorar y decidir sobre las solicitudes de la inclusión o no inclusión en el Registro Único de Víctimas.-Tramitar las solicitudes de novedades y/o actualizaciones.-Tramitar las diferentes órdenes judiciales allegadas a la Subdirección de Valoración y Registro (SVR).-Atender a las solicitudes de información, resolver los recursos y revocatorias interpuestos por las víctimas.-Tramitar las actuaciones administrativas correspondientes a presuntas víctimas que hayan ingresado al Registro Único de Víctimas de manera fraudulenta.-Generar documentos robustos, boletines, notas y otros productos a demanda que aporten a conocimiento, analítica y memoria institucional, asociada a los diferentes procesos misionales de la Unidad para las Víctimas.	Posibilidad de pérdida reputacional ante las víctimas y la entidad por alteración y difusión no autorizada de información que reposa en herramientas de gestión o activos físicos de información, debido a una administración inadecuada de perfiles de acceso a modificación o consulta o realizar modificaciones sin el conocimiento de los procedimientos establecidos.	Muy Alta	Mayor	Alto	El Agente General del Procedimiento de Gestión de de la Declaración realiza la actividad de forma diaria el registro y recepción de la documentación en el archivo Excel "ENTRGA DOCUMENTAL" en donde se registra una base de recepción y una base inicial de la documentación que ingresa para su tramite. **Evidencia:** Archivo de Excel ENTRGA DOCUMENTAL y/o envió de correo de notificación sobre los hallazgos. **(A.6.8, A.6.8, A.18.2.2, A.5.36)** El líder del procedimiento reporta que realiza actualizaciones de información RUV mensualmente informan sobre los requerimientos o solicitudes atendidas internamente al aplicativo ARANDA, esto con el fin de monitorear constantemente los incidentes presentados por parte del personal del operador y cuáles son las actualizaciones de información en el RUV que se presentan en el registro. Esto aplica para las solicitudes que se registren por medio de este aplicativo. en caso de encontrar tipologías de solicitudes nuevas, se realizara mesa de trabajo para identificar ruta de envió o generación de nueva tipología. **Evidencia:** Reporte mensual de los Ticket gestionados por ARANDA. **(A.6.8, A.6.8, A.18.2.2, A.5.36)** El Líder de cada procedimiento cada vez que se requiera carga la data de producción en la carpeta de SharePoint y/o OneDrive designada para el resguardo, para llevar la trazabilidad de los usuarios que cargue, modifican y eliminan información, esto con el fin de tener un control de información relacionada con quien tiene a cargo la información del proceso y los tiempos que la tiene a su cargo. En caso de requerir permisos en SharePoint se realiza la solicitud cada equipo de trabajo a la Oficina de Tecnologías y de Información -OTI. **Evidencia:** Data de producción por cada procedimiento y/o correo de solicitud de accesos a las carpetas de SharePoint. **(A.8.13)** El equipo de apoyo procedimiento gestión de la declaración brinda apoyo técnico a los funcionarios del Ministerio público o consulados en cuanto al uso adecuado de la herramienta de toma en línea, este acompañamiento se realiza por medio telefónico, correo electrónico, de atención inmediata. en caso de no poder contactar por alguno de estos medios, la entidad dispone de videos tutoriales para que se realice la toma de declaración en línea de manera adecuada y se informara de estos a la oficina que solicite asistencia. **Evidencia:** Correos Electrónicos, registro Formato seguimiento soporte en línea. **(A.6.3)**	**Moderado**	Reducir - Mitigación	El enlace del SIG de registro y valoración articula con la oficina de tecnologías de la información el desarrollo de una sensibilización en temas de seguridad de la información en articulación con la oficina de tecnologías de la información por medio de capacitaciones o material informativo, esto con el fin de que todos los colaboradores conozcan y se sensibilicen frente al manejo de la información con la que cuenta el proceso y los riesgos a los que se encuentra sujeto el mismo **Evidencia:** acta de reunión de los espacios de sesión y/o material divulga, en caso de no realice los espacios de socialización se genera un correo o documento que indique que no se presento en el periodo. **(A.6.3)**

CONTROL DE CAMBIOS.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Adriana Ximena Florez Martinez Adriana Florez M. **Cargo:** Contratista	**Nombre:** Dario Eduardo Muneton Zuluaga **Cargo:** Jefe de Oficina de Tecnología de la información – OTI	Comité Institucional de Gestión y desempeño **Acta:** **Fecha:**