El futuro es de todos

Unidad para la atención y reparación integral a las víctimas

Plan de tratamiento riesgos de seguridad de la información 2020.

TABLA DE CONTENIDO

Contenido

1. INTRODUCCIÓN

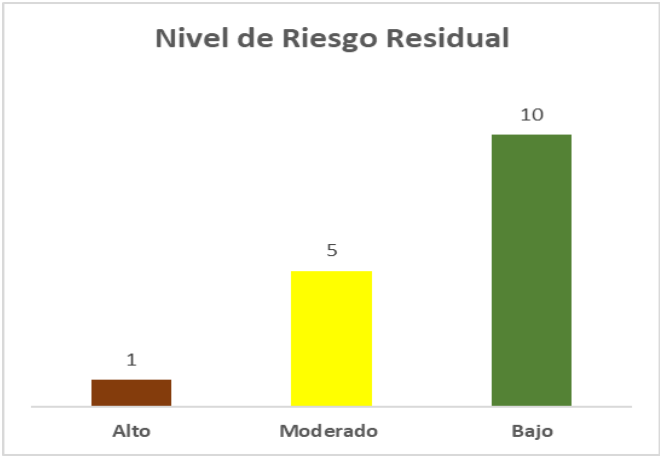
En el presente documento se encuentran consolidados los planes de tratamiento a los riesgos de seguridad de la información (incluyendo seguridad digital), identificados por los procesos a nivel central, que**,** de acuerdo con la metodología de administración de riesgos, establecida en la Entidad, se diseñan a partir de los riesgos con nivel residual valorado como moderado, alto y extremo. Esto debido a que, según la metodología establecida, cualquier riesgo cuya valoración a nivel residual sea superior a bajo debe contar con su correspondiente plan de tratamiento.

2. OBJETIVO

Establecer el plan de tratamiento a los riesgos identificados con la participación de los procesos Estratégicos, Misionales y de Apoyo, a partir la previa identificación de activos considerados críticos en términos de confidencialidad, integridad y disponibilidad. Permitiendo así, la identificación de las actividades específicas, a las cuales se les realice el correspondiente seguimiento y verificación del cumplimiento por parte de sus correspondientes responsables, en el marco de la metodología para la administración de riesgos definida por la Entidad.

3. ALCANCE

La identificación del plan de tratamiento de riesgos se realiza con base en los activos críticos[1] de información, previamente valorados y categorizados por cada proceso de la Entidad, con base al procedimiento de “Generación del inventario de activos de información”, establecido en el marco del Sistema Integrado de Gestión (SIG). De esta manera, la gestión de riesgos permite identificar específicamente el activo de información que será afectado y los controles establecidos para mitigar su riesgo inherente, para determinar el nivel de riego residual, cuyo nivel establece si se requiere diseñar el respectivo plan de tratamiento. A continuación, se relacionan la cantidad de riesgos categorizados por el nivel de riesgo residual:



[1] Se considera activo crítico cuando, en el inventario de activos de información, su valoración de impacto en términos de Confidencialidad, Integridad y Disponibilidad se estima en nivel cuatro (4) o cinco (5), según el procedimiento establecido para la generación del inventario de activos de información. El activo que se considera crítico hace parte del alcance en la gestión de riesgos de seguridad de la información, con base en la metodología de administración de riesgos establecida en la Unidad.

4. ACTIVIDADES

A continuación, se presentan los planes de tratamiento al riesgo de los procesos que de acuerdo con la calificación de riesgo residual se encuentran en nivel: alto y Moderado, y en consecuencia requieren la definición y ejecución del plan de tratamiento al riesgo.

4.1. Planes de tratamiento de riesgos de seguridad de la información por proceso

La unidad cuenta con una matriz de riesgos de seguridad de la información y seguridad digital, que aplica a los procesos en el nivel central, la cual se encuentra en la ruta https://www.unidadvictimas.gov.co/es/mapa-de-riesgos-institucional-corrupcion-y-gestion-2020-v2/57993.

A continuación, se presenta la información con respecto los planes de tratamiento a los riesgos identificados de los 6 procesos, una vez realizado su análisis y evaluación de riesgo se encuentran en una zona residual moderado, alto y extrema.

4.1.1. Registro y valoración

IDENTIFICACIÓN		VALORACIÓN		
Causas/ Vulnerabilidades	Riesgo	Riesgo Inherente	CONTROLES	Riesgo Residual
		Zona de Riesgo	Descripción	Zona de Riesgo
Falta de conciencia acerca de la seguridad	Pérdida parcial o total de la Confidencialidad, integridad y/o Disponibilidad de los sistemas de información y/o la información registrada en documento físico o digital.	Extrema	El enlace del SIG de registro y valoración cada vez que se requiera, realizará 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 (inforgrafias), principalmente cuando se genere el ingreso de nuevo personal al proceso, esto con el fin de que todos los colaboradores conoczcan y se sencibilicen frente al manejo de la informacion con la que cuenta el proceso y los riesgos a los que se enceuntra sujeto el mismo. Evidencia: Correos electrónicos o medios de socialización y/o actas y listas de asistencia.	Moderada
Ausencia de mecanismos de monitoreo			El grupo de sistemas del operador de Registro y valoración mensualmente informará sobre los requerimientos o solicitudes atendidas internamente el aplicativo aranda, esto con el fin de monitorear constantemente los incidentes presentados por parte del personal del operador y cuales son las novedades o actualizaciones que se presentan en el registro. Esto aplica para las solicitudes que se registren por medio de este aplicativo. Evidencia: Reporte mensual de los Ticket gestionados por el grupo de sistemas del operador.	
Descarga y uso no controlados de software			El Líder de cada procedimiento semanalmente cargará la data de producción en la carpeta de SharePoint, herramienta la cual refleja la trazabilidad de los usuarios en el cargue, modificación y eliminación de archivos, esto con el fin de tener un control de informacion relacionadado con quien tene a cargo la informacion del proceso y los tiempos que la tiene a su cargo asi como, los permisos de cada carpeta los manejará la Oficina de Tecnologías y de Información -OTI. Evidencia; Carpeta SharePonit por cada procedimiento, correo de solicitud de accesos a las carpetas.	
Ausencia de copias de respaldo				
Herramienta toma en linea no permite el cambio de contraseña de forma periodica por parte del usuario (uso seguro de contraseñas).			El equipo de apoyo procedimiento gestión de la declaración brindará 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 y vía Skype 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.	
inadecuado uso de la herramienta toma en linea que deriva en no finalizar la declaracion de forma correcta.				

PLAN DE TRATAMIENTO AL RIESGO				
Acción	**Fecha de Inicio** (A partir de esa fecha se debe llevar a cabo la acción)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	**ACCION SI EL RIESGO SE MATERIALIZA**
Socializar al interior de cada proceso los productos presentados en el marco de los encuentros de enlaces SIG y/o los boletines o flash informativos que se generen en materia de seguridad de la información.	15/07/2020	5 meses	Enlace SIG en articulación con la OTI	El proceso de registro y valoración a través de la línea de mesa de servicio de gestión de requerimientos técnicos, una vez identificada la necesidad, reporta a la mesa de servicios tecnológicos incidencias que se presentan en las herramientas de consulta a través de los canales acordados con la OTI.
Se realizará con el acompañamiento de la OTI una socialización sobre el almacenamiento de la información con ONE -DRIVE, para mantener la información protegida de manera permanente.	15/07/2020	5 meses	Enlace SIG en articulación con la OTI	
Desarrollar mesas de trabajo con RNI con el fin de validar la implementacion de módulo de modificacion y/o recordatorio de contraseñas y log de auditoría en el aplicativo Toma en Linea, Cumpliendo con las políticas del SGSI y que se aplique tanto a la versión central como a la versión de escritorio.	31/07/2020	5 meses	Lider de procedimeinto Gestion de la delcaracion y Enlace SIG	

4.1.2. Reparacion Integral

IDENTIFICACIÓN		CONTROLES		
Causas/ Vulnerabilidades	**Riesgo**	**Riesgo inherente** Zona de Riesgo	**Descripción**	**Riesgo Residual** Zona de Riesgo
Vandalismo o hurto, por ausencia o insuficiencia de controles de acceso al archivo digital.	"Pérdida parcial o total de la Confidencialidad, integridad y/o Disponibilidad 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."	**Extrema**	Los Administradores de los Sistemas de información del proceso Reparación Integral, permanentemente cuentan con formularios de inicio de sesión que sólo permiten el acceso a la información de la Dirección de Reparación a través de un usuario de autenticación como de una contraseña segura, de lo contrario no se tendrá acceso a las mismas. Este usuario se asigna mediante la suscripción de un acuerdo de confidencialidad. Como evidencia se cuenta con la relación mensual de usuarios de las herramientas y los acuerdos de confidencialidad suscritos.	**Moderada**
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.			Los administradores de las herramientas tecnológicas del Proceso Reparación Integral cuentan con monitoreos mensuales de las fechas y horas de ingreso a las herramientas que permiten identificar los accesos de los usuarios a las herramientas, donde se busca identificar casos inusuales. En caso de ingresos sospechosos se realiza el bloqueo de los usuarios y se adelanta la investigación. Como evidencia tenemos los informes mensuales de seguimiento de los aplicativos.	
Acceso no controlado a información sensible / confidencial.			Los administradores de la herramientas tecnológicas del Proceso Reparación integral, suscriben el "ACUERDO DE CONFIDENCIALIDAD DE USUARIOS DE HERRAMIENTAS TECNOLÓGICAS O INFORMACIÓN DE LA UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS", cada vez que se solicitan usuarios de las herramientas. De lo contrario no se asignarán los usuarios. En caso que se venza el acuerdo, el usuario es deshabilitado. Como evidencias se cuenta con los acuerdos de confidencialidad suscritos por cada herramienta y la inhabilitación de usuarios.	
Desconocimiento de los procedimientos y controles de Seguridad de la Información.			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. Como evidencia tenemos pantallazos de los sistemas de validación implementados en las herramientas.	
Omisión o inadecuado proceso de identificación y calificación de los activos de información.			Las dependencias de la Dirección de Reparación por medio de los enlaces definidos, realizan dos revisiones anuales para la identificación, calificación y actualización de los activos de la información asociados al proceso Reparación Integral, de acuerdo con los lineamientos del Proceso Gestión de la información y el procedimiento e instructivo definido. Cómo evidencia tenemos correos electrónicos con la revisión y el inventario de activos de la información revisado y actualizado.	

PLANES DE TRATAMIENTO AL RIESGO					ACCION SI EL RIESGO SE MATERIALIZA
Acción	**Meta** (cantidad y periodicidad)	**Fecha de Inicio** (A partir de esa fecha se debe llevar a cabo la acción)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	
Sensibilizar a los colaboradores para que hagan uso responsable en el acceso y manejo de la información de la Dirección de Reparación.	Realizar procesos de sensibilización y socialización a funcionarios sobre uso de la información (Por lo menos uno mensual).	1/07/2020	12 Meses	Equipo Control y Seguimiento - Dirección de Reparación - OTI.	Verificar las copias de seguridad con las que cuenta la Unidad Para las Víctimas (digitales y físicos) y realizar la reconstrucción de la información faltante.
Implementar nuevas acciones de seguridad para el uso de los sistemas de información de la Dirección de Reparación en articulación de la Oficina de Tecnologías de Información.	Dos acciones, controles y/o mejoras, nuevas de seguridad.	1/07/2020	12 Meses	Equipo Control y Seguimiento - Dirección de Reparación	
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.	A demanda de la OTI.	1/07/2020	12 Meses	Equipo Control y Seguimiento - Dirección de Reparación	
Promover el etiquetado de información con Enterprise Mobility Security (EMS) de Microsoft, aplicado a Word, Excel, PowerPoint y Access, herramienta que provee el Office 365 con el Windows 10.	Realizar 2 procesos de sensibilización y socialización a funcionarios sobre Enterprise Mobility Security (EMS)	1/07/2020	12 Meses	Enlace SIG Reparación Integral.	

4.1.3. Gestión Jurídica

IDENTIFICACIÓN		CONTROLES		
Causas/ Vulnerabilidades	**Riesgo**	**Riesgo Inherente** **Zona de Riesgo**	**Descripción**	**Riesgo Residual** **Zona de Riesgo**
Falta de herramienta o aplicativo para almacenar la informacion del proceso y sus grupos de trabajo.	Pérdida parcial o total de la Confidencialidad, integridad y/o Disponibilidad de los sistemas de información y/o la información registrada en documento físico o digital (OJ - AAC- 001, OJ - AAC- 005, OJ - DFJ – 001, OJ - DFJ – 002, OJ - DFJ – 003, OJ - DFJ – 005, OJ - DFJ – 006, OJ - DFJ – 007, OJ-JEF-005, OJ - AA- 019, OJ - DF – 008, OJ - DF – 009, OJ - DF – 010, OJ - DF – 011, OJ - DF – 012, OJ-JEF-001, OJ-JEF-002, OJ-JEF-003, OJ-JEF-004, OJ-GRJ-001, OJ-GRJ-002, OJ-GRJ-004, OJ-GRJ-005, OJ - AA- 020, OJ - AA- 021, OJ-GRJ-006, OJ - AA- 022,OJ-JEF-005, OJ-GRJ-006, OJ - DF – 013, OJ - AA- 023)	Alta	Los administrativos de Actuaciones administrativas, de defensa judicial, y gestión normativa y conceptos realizan copia de seguridad en OneDrive de las bases de datos utilizadas como herramienta de consulta y actualización de estado de los procesos o de información, con el objetivo de tener una copia actualizada de las bases de datos y evitar la pérdida de información general de los grupos de trabajo, esta copia se realiza directamente de las bases de datos actualizadas a diario. En caso de no realizarse el respaldo de la información cada coordinador debe remitir un correo de solicitud de esta actividad al administrativo. Queda de evidencia el respaldo de las bases de datos utilizadas por los grupos de trabajo de la Oficina Asesora Jurídica en la herramienta OneDrive dispuesta por la Unidad.	Moderada
Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.			Los administrativos de Actuaciones administrativas de defensa judicial, gestión normativa y conceptos suscriben el "Acuerdo De Confidencialidad de usuarios de acceso a las herramientas tecnológicas o Información de gestión de la Unidad Para La Atención Y Reparación Integral a las Víctimas", con una frecuencia anual o al momento de ingreso del contratista, por medio del acuerdo se realiza la solicitud de los usuarios de consulta de las herramientas misionales de la Unidad. Que tiene como objetivo asegurar la información consultada, controlar y hacer seguimiento de los usuarios que acceden a los aplicativos. En caso de no tener el debido acuerdo suscrito no se asignará los usuarios y en caso de que se venza el acuerdo el usuario es deshabilitado. Como evidencias se cuenta con los acuerdos de confidencialidad suscritos por cada herramienta en la carpeta destinada en Totoro	

PLAN DE TRATAMIENTO AL RIESGO				ACCION SI EL RIESGO SE MATERIALIZA
Acción	**Fecha de Inicio** (A partir de esa fecha se debe llevar a cabo la acción)	**Duración (**meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	
Gestionar el respaldo de la información de las bases de datos críticas en OneDrive, servidor de archivos Totoro y/o SharePoint de la Oficina Asesora Jurídica.	1/08/2020	5 meses	Jefe de la Oficina Asesora Jurídica	Gestionar con la Oficina de tecnologías de la Información un reporte periodico de los usuarios activos del proceso, para validar, aprobar o realizar la inactivación oportuna de credenciales de acceso a sistemas de información.
Realizar reunion con la OTI para gestionar el aplicativo tecnológico en la Entidad para la consulta y control de la informacion de los grupos de trabajo de la Oficina Asesora Jurídica	1/08/2020	5 meses	Jefe de la Oficina Asesora Jurídica	

4.1.4. Gestión de talento humano

IDENTIFICACIÓN		CONTROLES		
Causas/ Vulnerabilidades	**Riesgo**	**Riesgo Inherente** Zona de Riesgo	**Descripción**	**Riesgo residual** Zona de Riesgo
Insuficiencia de controles de acceso a las instalaciones	Pérdida total o parcial de la confidencialidad y/o integridad de la información almacenada en sistemas de información físico o digital considerado crítico, debido a la divulgación, pérdida y/o alteración de la información personal y/o laboral de los funcionarios activos y/o retirados de la Unidad. (TH-COP-001,TH-SST-007,TH-HLF-010,TH-SST-012,TH-SST-013,TH-VIN-030,TH-NOM-030)	Alta	El funcionario responsable de las historias laborales diligencia a diario los registros para el control de la custodia y contenido de los expedientes, identificando fecha, responsable, contenido y folios de los documentos manipulados. En caso de identificar faltantes o alteraciones requerirá formalmente al último responsable registrado e informará a la Coordinación de Talento Humano las demoras o inconsistencias en las respuestas para que se adelanten las investigaciones pertinentes. Evidencia: Formato préstamo de documentos (710.14,15-13) y Formato hoja de control de expedientes de historias laborales (710.14.15-33)	Moderada
Ausencia de mecanismos de digitalización o herramientas de sistematización que brinden respaldo a la información			El funcionario responsable de las historias laborales diligencia a diario los registros para el control de la custodia y contenido de los expedientes, identificando fecha, responsable, contenido y folios de los documentos manipulados. En caso de identificar faltantes o alteraciones requerirá formalmente al último responsable registrado e informará a la Coordinación de Talento Humano las demoras o inconsistencias en las respuestas para que se adelanten las investigaciones pertinentes. Evidencia: Formato préstamo de documentos (710.14,15-13) y Formato hoja de control de expedientes de historias laborales (710.14.15-33)	
Insuficiente personal capacitado y con responsabilidades específicas en la custodia de expedientes			El grupo de Gestión administrativa y documental presta el apoyo diariamente a la custodia de los expedientes laborales de los funcionarios de la Unidad, El grupo de Talento Humano una vez se cuente con la documentación completa por cada expediente laboral, entrega los expedientes para custodia, el Grupo de gestión Administrativa realiza la recepción del documentación, realizando el check list respectivo por cada historia laboral, en los que casos que la documentación se encuentre incompleta el funcionario del Grupo de gestión administrativa procede a devolver todo el expediente laboral para revisión y ajuste por parte del Grupo de gestión de Talento Humano, Evidencia: Formato listado de requisitos(770,12,15-61), Formato hoja de control de expedientes de historias laborales (710.14.15-33).	

PLAN DE TRATAMIENTO AL RIESGO					ACCION SI EL RIESGO SE MATERIALIZA
Acción	**Meta** (cantidad y periodicidad)	**Fecha de Inicio** (A partir de esa fecha se debe llevar a cabo la acción)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	
Implementar herramienta tecnológica que permita la digitalización de las historia laborales, esto permite reducir a manipulación de la historias laborales de los funcionarios y a su vez el riesgo de pérdida de los documentos.	80% de los expedientes laborales de los funcionarios de la Unidad para las victimas digitalizados.	1/10/2020	12 meses	Coordinador Talento Humano	Realizar verificación exhaustiva de la trazabilidad y control del documento y de confirmarse la materialización, poner en conocimiento de las instancias competentes.
Implementar modulo de hojas de vida en la herramienta tecnológica de administración de planta de Talento Humano que fortalezcan la administración y control de historias laborales	1 modulo de hoja de vida implementado y en funcionamiento en la herramienta tecnológica para la administración y control de historias laborales	1/10/2020	12 meses	Coordinador Talento Humano	
Realizar capacitación al personal de Talento Humano que gestiona y custodia los expedientes laborales de los funcionarios de la Unidad, sobre el manejo de los expedientes y disposición de los mismos	2 capacitaciones anuales	1/02/2021	10 meses	Coordinador Talento Humano	

4.1.5. Gestión de Información

IDENTIFICACIÓN		CONTROLES		
Causas/ Vulnerabilidades	**Riesgo**	**RIESGO INHERENTE** Zona de Riesgo	**Descripción**	**RIESGO RESIDUAL** Zona de Riesgo
Ausencia o insuficiencia de procedimientos de Monitoreo de los recursos de procesamiento de información.	Indisponibilidad y/o perdida y/o modificación no controlada de la información almacenada en sistemas de información considerados criticos y que son custodiados por la oficina de tecnologías de la información TI-SIF-001, TI-SIF-002, TI-SIF-003, TI-SIF-004, TI-SIF-005, TI-SIF-006, TI-SIF-007, TI-SIF-008, TI-SIF-009, TI-SIF-010, TI-SIF-011, TI-SIF-012, TI-SIF-013, TI-SIF-014, TI-SIF-015, TI-SIF-018, TI-SIF-019, TI-SIF-022, TI-SIF-023, TI-SIF-024, TI-SIF-025, TI-SIF-031	Moderada	El equipo de infraestructura realiza el monitoreo frecuente de la capacidad disponible de almacenamiento en servidores de aplicación, bases de datos y File Servers, así como de los canales de conectividad, a través de las herramientas establecidas para tal fin con una frecuencia diaria, con el fin de controlar y racionalizar la capacidad tecnológica En caso de identificar la necesidad de mejorar la capacidad del recurso tecnológico, se realiza la correspondiente solicitud al proveedor siempre y cuando este dentro de la capacidad establecida. La evidencia es la operación de la herramienta para el monitoreo en tiempo real de los servidores	Moderada
Falla, daño o degradación de equipos.			La responsable de servicios TI-soporte tecnológico gestiona la ejecución del mantenimiento preventivo anual de los equipos de computo de la Unidad, susceptibles de ser realizados dada la emergencia por el COVID-19, por lo que se desplaza un técnico de soporte y realiza el mantenimiento en sitio de cada equipo que se encuentre en las sedes, lo que permite prevenir fallas de los mismos, dejando como evidencia la firma de un acta por parte del soporte en sitio que recibe el mantenimiento en sede nacional y en territorio la persona que se designe el director territorial, dada la emergencia que se presenta y que el usuario no se encuentra en el sitio . En caso de que se presenten fallas posterior al mantenimiento y de que el usuario realice el uso remoto de la maquina, deberá informarse a soporte tecnológico por los medios divulgados duramte el periodo de aislamiento.	
Acceso no controlado a información sensible / confidencial.			El equipo de sistemas de información implementa usuario y clave a los sistemas de información que gestionan información no publica con el fin de controlar el acceso a aplicativos. La frecuencia de implementación es por demanda según solicitudes de desarrollo y su evidencia es la funcionalidad implementada en el sistema de información. En caso de que no se implemente este control la aplicación no se lleva a producción	
Debilidades de los sistemas de información frente a requisitos de seguridad y privacidad de la información			El equipo de seguridad y privacidad de la información, el equipo de desarrollo de sistemas de información y los lideres técnicos de sistemas de información priorizados, diligencian la lista de verificación de requisitos de seguridad de los sistemas de información críticos existentes con una frecuencia anual, con el fin de valorar y establecer el estado de los sistemas de información en términos de seguridad. En caso de que no se diligencie se escala al lider del proceso al que pertenece el sistema de información para solicitar el diligenciamiento y en caso de que no se logre se crea una no conformidad al proceso que no atiende la solicitud . Como evidencia se cuenta con la lista de verificación diligenciada y evidencia de las acciones tomadas en caso de desviaciones si aplica.	
Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.				

PLAN DE TRATAMIENTO AL RIESGO					ACCION SI EL RIESGO SE MATERIALIZA
Acción	**Meta** (cantidad y periodicidad)	**Fecha de Inicio** (A partir de esa fecha se debe llevar a cabo la acción)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	
Actualizar el procedimiento de seguridad de la información, conforme a: 1) resultado de la consultoría 2019, 2)los lineamientos de MinTIC y del MIPG que apliquen, según disponibilidad de recursos y que sean susceptibles de ser implementados de acuerdo a la estrategía que se defina en la OTI para este fin.	1 Procedimiento actualizado Aplicación por demanda según necesidades de actualización de procedimiento	1/06/2020	9 meses	-Responsable del dominio de seguridad de la información -Responsable de gestión de calidad y cumplimiento OTI	Implementar el procedimiento de gestión de incidentes, creación de no conformidades y escalamiento a las autoridades competentes si aplica
Actualizar lineamientos del dominio de seguridad de la información en el marco del dominio de gobierno TI	1 Documento de lineamientos de seguridad de la información (Por demanda según se requiera la actualización)	1/07/2020	12 meses	-Responsable dominio de gobierno TI y -Responsable dominio de sistemas de información	
Automatizar y socializar el proceso para atender el desarrollo de sistemas de información, conforme a los nuevos lineamientos de MinTIC aplicables, manteniendo la trazabilidad y auditoria de transacciones, criterios minimos para requerimientos funcionales y no funcionales, Identificar los controles de seguridad relacionados con el ciclo de vida de la gestión de usuarios en sistemas de información, entre otros.	1 Procedimiento actualizado conforme a la automatización del proceso de desarrollo. Aplicación por demanda según necesidad de actualización	1/06/2020	7 meses	-Responsable dominio de sistemas de información -Responsable gestión de calidad y cumplimiento.	

Identificación		Controles		
Causas/ Vulnerabilidades	Riesgo	Riesgo Inherente Zona de Riesgo	Descripción	Riesgo Residual Zona de Riesgo
Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.	Divulgación, modificación, extracción y/o destrucción de manera accidental y/o deliberada de la información de gestión por parte del personal (recurso humano) del proceso, que es considerada critica para la operación. TI-ARH-001, TI-ARH-002, TI-ARH-003, TI-ARH-005, TI-ARH-007, TI-ARH-008, TI-ARH-010	Baja	El equipo de seguridad y privacidad de la información, por medio de un análisis avanzado sobre los casos atípicos que se presenten con la cuenta de dominio asignada por la entidad a los usuarios, realiza el monitoreo de amenazas con una periodicidad mensual, con el fin de prevenir riesgos de seguridad frente al personal. La evidencia consiste en los correos de los tickets resueltos remitidos por la mesa de servicios tecnológicos frente a los casos creados por parte del equipo de seguridad en función del resultado del análisis. En caso de fallos frente a este control se realiza el diagnostico y análisis de la situación y se toman acciones puntuales para atenderla.	Baja
Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los empleados y/o terceras partes.			El equipo de seguridad y privacidad de la información, con una frecuencia establecida según la demanda o solicitud, apoya los procesos contractuales, revisando los documentos de estudios previos y anexos técnicos y sugiriendo clausulas relacionadas con el aseguramiento de la información, con el fin de atender las necesidades de la Unidad en cuanto a la implementación de seguridad de la información y digital. En caso de presentarse desviaciones en cuanto las cláusulas y/o sugerencias del equipo de seguridad, se toman acciones técnicas o administrativas requeridas. Como evidencia se cuenta con las respuestas a la revisión por parte del equipo de seguridad y soportes en caso de desviaciones si aplica.	
Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.			El equipo de infraestructura de la Oficina de Tecnologías de la Información, implementa el procedimiento de acceso remoto a servidores y bases de datos, con el fin de controlar de acceso a servidores teniendo en cuenta las IPs autorizadas, que aplica unicamente a la necesidad del equipo de Sistemas de Información y soporte aplicaciones, según solicitud por demanda. Cómo evidencia se generan los registros del procedimiento establecido. En caso de fallos frente a este control se realiza el diagnostico y análisis de la situación y se toman acciones puntuales para atenderla.	

Identificación		Controles		
Causas/ Vulnerabilidades	Riesgo	Riesgo Inherente Zona de Riesgo	Descripción	Riesgo Residual Zona de Riesgo
Acceso no controlado a información sensible / confidencial.	Divulgación, modificación, extracción y/o destrucción de manera accidental y/o deliberada de la información de gestión por parte del personal (recurso humano) del proceso, que es considerada critica para la operación. TI-ARH-001, TI-ARH-002, TI-ARH-003, TI-ARH-005, TI-ARH-007, TI-ARH-008, TI-ARH-010	Baja	Cada administrador funcional de los sistemas de información es el responsable de la creación, modificación o inactivación de credenciales de acceso de usuarios del aplicativo a su cargo o en su defecto el autorizado delegado por parte de la Dirección General, con base en las solicitudes que reciba por parte de los lideres del proceso según lo establecido en el procedimiento de creación de usuarios, para controlar los permisos y el acceso de los usuarios a las aplicaciones del alcance del procedimiento. La frecuencia depende de la demanda de solicitudes, y como evidencia se cuenta con los registros de solicitudes de creación de usuario. En caso de no implementarse se realiza el diagnostico identificando el responsable de la asignación de permisos y se toman acciones puntuales administrativas, legales y/o técnicas para atenderla.	Baja
Inoportunidad en la información remitida por parte de talento humano y/o de contratos respecto a los colaboradores que ingresan o se retiran de la entidad, de manera que se crean cuentas de correo mas tarde de lo esperado por el usuario o se eliminan cuentas en un tiempo mayor al adecuado para la Unidad.				

Plan de tratamiento al riesgo					ACCION SI EL RIESGO SE MATERIALIZA
Acción	**Meta** (cantidad y periodicidad)	**Fecha de Inicio** (A partir de esa fecha se debe llevar a cabo la acción)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	
Actualizar el procedimiento de seguridad de la información, conforme a: 1) resultado de la consultoría 2019, 2)los lineamientos de MinTIC y del MIPG que apliquen según disponibilidad de recursos y sean suceptibles de ser implementados de acuerdo a la estrategía que se defina en la OTI para este fin.	1 Procedimiento actualizado Aplicación por demanda según necesidades de actualización de procedimiento	1/06/2020	9 meses	-Responsable del dominio de seguridad de la información -Responsable de gestión de calidad y cumplimiento OTI	Realizar la investigación que permita diagnosticar la causa y tomar acción inmediata técnica, judicial o administrativa para corregir la situación
Actualizar lineamientos del dominio de seguridad de la información en el marco del dominio de gobierno TI	1 Documento de lineamientos de seguridad de la información (Por demanda según se requiera la actualización)	1/07/2020	12 meses	-Responsable dominio de gobierno TI y -Responsable dominio de seguridad de la información	
Realizar un ejercicio de ingeniería social través de la modalidad de phishing o Vishing controlado como ejercicio de sensibilización a los usuarios de la Entidad.	1 Ejercicio de ingenieria social controlado (periodicidad según disponibilidad de recurso humano)	1/09/2020	12	-Responsable dominio de seguridad de la información	

4.1.6. Gestión para la Asistencia

IDENTIFICACIÓN		CONTROLES		
Causas/ Vulnerabilidades	**Riesgo**	**Riesgo Inherente** Zona de Riesgo	**Descripción**	**Riesgo Residual** Zona de Riesgo
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.	Pérdida parcial o total de la Confidencialidad, integridad y/o disponibilidad de los sistemas de información y/o la información registrada en documento físico o digital. Disponibilidad de los sistemas deinformación y/o la informaciónregistrada en documento físico o digital. GA-BDD-007 - GA- BMT-011 - GA-BSM-012	Extrema	La Subdirección de Asistencia y Atención Humanitaria, a través de la línea de acción de administración y gestión de sistemas de información, suscriben el "Acuerdo De Confidencialidad De Usuarios De Herramientas Tecnológicas O Información De La Unidad Para La Atención Y Reparación Integral A Las Víctimas", cada vez que se solicitan usuarios de las herramientas. De lo contrario no se asignarán los usuarios. En caso de que se venza el acuerdo, el usuario es deshabilitado. Como evidencia se cuenta con los formatos de aceptación de acuerdos.	Alta
Acceso no controlado a información sensible / confidencial..			La Subdirección de Asistencia y Atención Humanitaria, a través de la línea de acción de administración y gestión de sistemas de información, suscriben el "Acuerdo De Confidencialidad De Usuarios De Herramientas Tecnológicas O Información De La Unidad Para La Atención Y Reparación Integral A Las Víctimas", cada vez que se solicitan usuarios de las herramientas suministrando horarios de acceso para VIVANTO, así cómo también, que la URL de acceso a la herramienta de SM donde se activan las mediciones y se realizan las gestiones de pagos, solo se encuentran disponible estando conectado a la Red de la Unidad . De lo contrario no se asignarán los usuarios. En caso de que se venza el acuerdo, el usuario es deshabilitado. Como evidencia se cuenta con los formatos de aceptación de acuerdos.	
Falta o deficiencia de sistemas automatizados para ejecutar procesos			La Subdirección de Asistencia y Atención Humanitaria, a través de la línea de acción de Gestión para la Entrega de asistencia humanitaria, consolida a través de bases de acceso la colocación de las solicitudes de ayuda humanitaria que se aprueban previamente a través del análisis de información y cumplimiento de los requisitos definidos en la resolución 2349 de 2012, cada vez que se solicita realizar colocaciones y realizan las gestiones de pagos. Como evidencia se cuenta con las bases acceso del trámite realizado que se encuentra en un equipo de cómputo de la Unidad.	
Envío de información sensible en anexos en excel por el correo				

PLAN DE TRATAMIENTO AL RIESGO				
Acción	**Fecha de Inicio** (A partir de esa fecha se debe llevar a cabo la acción)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable (cargo)**	**ACCION SI EL RIESGO SE MATERIALIZA**
Inactivar oportunamente las credenciales de acceso a los sistemas de información a través de la documentación establecida para tal fin, cada vez que se identifica la desvinculación de las personas que hacen parte de la operación relacionada con la prestación de los servicios del proceso, con la finalidad de evitar el acceso no autorizado de la información y su confidencialidad. Esta actividad es realizada por la Subdirección de Asistencia y Atención Humanitaria, a través de la línea de acción de administración y gestión de sistemas de información.Como evidencias se cuenta con los correos de los tiquets a mesa de servicio.	Julio de 2020	6 meses	Director del Proceso	La Subdirección de Asistencia y Atención Humanitaria a través de la línea de acción administración y gestión de sistemas de información, una vez identificada la necesidad, reporta a la mesa de servicios tecnológicos las caídas o errores que se presentan en las herramientas de consulta a través del aplicativo ARANDA a la OTI.

Proyectó	Marcela Rocio Torres Saboyà	
Revisó	Joaquin Rojas Palomino	
Aprobó por parte de la OTI	Ingeniero Victor Duran	

DOCUMENTO DE REFERENCIA

1. Metodología administración de riesgos V8
2. Formato Levantamiento Mapa de Riesgos V7

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
	Octubre 2020	Versión 1.0