 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 1 de 19

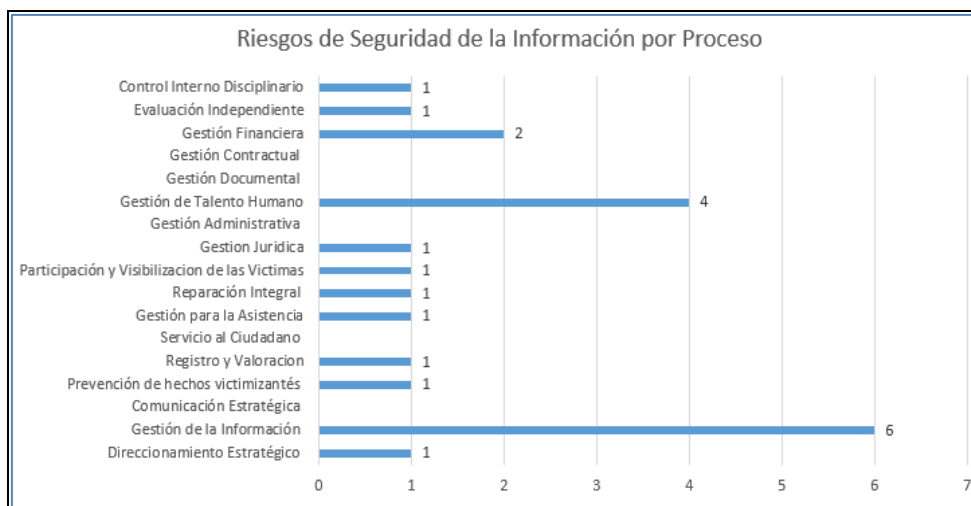
1. OBJETIVO:

El objetivo del presente documento es consolidar los planes de tratamiento de riesgos de seguridad de la información, generados por los procesos de la Entidad en el marco de la metodología establecida para la administración de riesgos, asociados a los activos críticos previamente identificados.

2. ALCANCE:

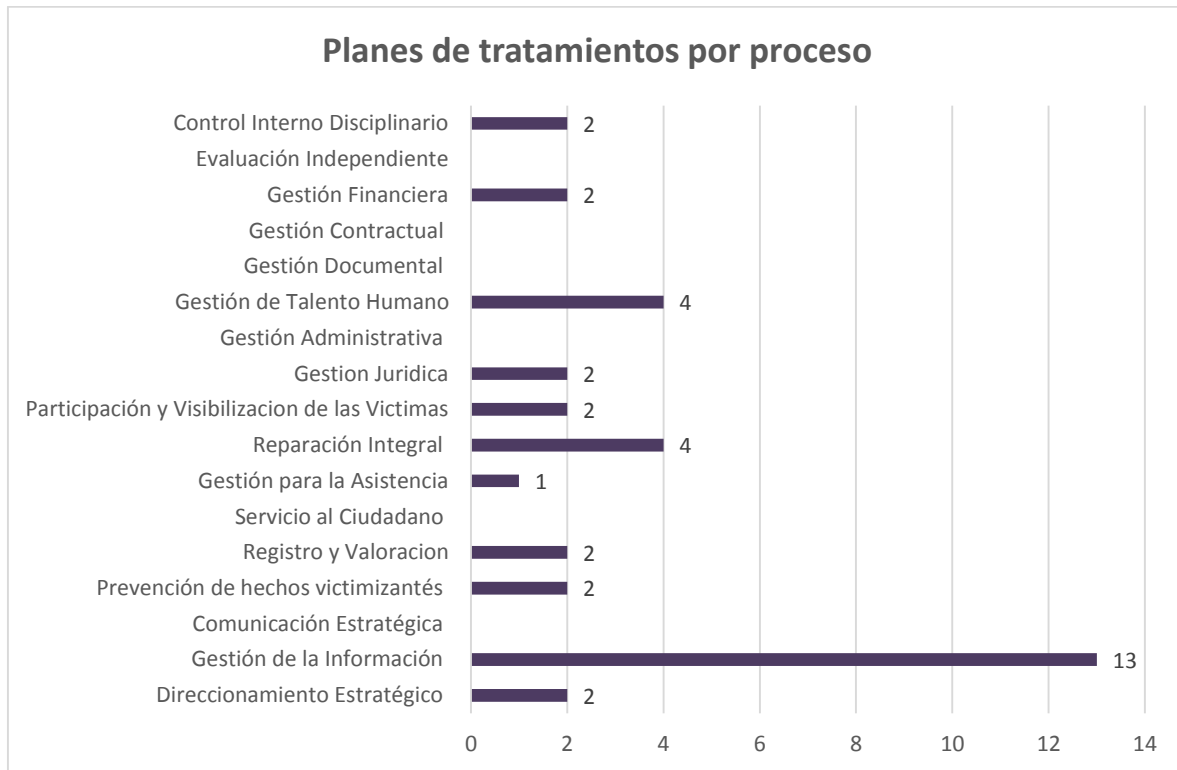
Los riesgos de seguridad de información actualmente identificados se encuentran asociados a los activos críticos de información identificados, valorados y categorizados por cada proceso de la Entidad, con base al procedimiento de Generación de Inventario de activos de información con codificación 710.14.08-9, establecido en el marco del Sistema Integrado de Gestión. Esto con el objetivo de definir específicamente el activo de información que sería afectado y los controles establecidos para mitigar su riesgo inherente y así determinar el nivel de riesgo residual, lo cual permite determinar si se requiere diseñar el correspondiente plan de tratamiento.

Es importante mencionar que, si un activo identificado cuenta con una valoración entre cuatro (4) y cinco (5) en el campo “Impacto CID1”, se considera crítico y 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. A continuación, se relacionan los procesos y el número de riesgos identificados:



¹ El campo “Impacto CID”, hace referencia al promedio de impactos definidos en términos de confidencialidad, integridad y disponibilidad, en el formato “FORMATO REGISTRO DE ACTIVOS DE INFORMACIÓN”, del procedimiento para la “GENERACIÓN DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN”

Una vez se identifica el valor del riesgo residual, se determina la necesidad de identificar el plan tratamiento de riesgos. A continuación, se identifican los planes de tratamiento identificados en cada proceso:




3. DEFINICIONES:

Activo de información²: Es la información que tiene valor para la organización y los elementos relacionados con la misma, como por ejemplo sistemas, elementos de hardware, personas e instalaciones.

Activo Crítico: Son Activos de información que, debido a la criticidad dentro de un proceso, y que además al realizar el promedio en la calificación de los tres pilares de seguridad de la información: confidencialidad, integridad y disponibilidad, se localice entre una escala del 4 al 5 se categoriza en activo crítico.

Amenaza: Las amenazas son todos los elementos o acciones capaces de atentar contra la seguridad de la información y son generadoras de eventos; Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada.


² Metodología de Administración de Riesgos -Unidad para las Víctimas-Definiciones

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018

Calificación de Riesgos: cuantificación de los riesgos de acuerdo con la probabilidad de ocurrencia o frecuencia y sus consecuencias.

Riesgo seguridad de la información: Hace referencia a la posibilidad de que una amenaza pueda explotar una vulnerabilidad de un activo de información, afectando la operación o la imagen de la Entidad.

Vulnerabilidad: Las vulnerabilidades son las debilidades inherentes al activo que lo hacen susceptible de ser atacado.


 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 4 de 19

4. ACTIVIDADES:

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


4.1.1. Gestión Financiera

	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001: 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. - Activo 1 (GF-TES-001) - Activo 2 (GF-TES-005) - Activo 3 (GF-TES-006) - Activo 4 (GF-TES-010) - Activo 5 (GF-TES-011)	Alta	Reducir	Se solicitará acompañamiento y capacitación para guardar la información en OneDrive.	1 solicitud	01/06/2018	Coordinador Gestión Financiera
RSEG003: Pérdida de confidencialidad, integridad o disponibilidad ocasionada por la infiltración en el servidor, en el dispositivo de red y/o el sistema de información, debido al acceso no autorizado como consecuencia de captura de credenciales transferidas en texto claro, durante el ingreso vía web. - Activo 1 (GF-IMP-011) - Activo 2 (GF-GFI-014)	Alta	Reducir	Se realizará la socialización al interior del proceso flash y boletines informativos sobre temas de seguridad de la información	3 flash y boletines informativos socializados	01/06/2018	Coordinador Gestión Financiera

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 5 de 19


4.1.2. Direccionamiento Estratégico

	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001: 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. Activos : DE-GVE-031 y DE-GVE-032	Moderada	Reducir	Gestionar el respaldo de la información almacenada en equipos de cómputo asignados al usuario, teniendo en cuenta OneDrive o servidor de archivos Totoro.	1 gestión de copias de respaldo y/o almacenamiento.	01/06/2018	Enlaces SIG del proceso (Dirección General, Subdirección general, Oficina de Planeación, Cooperación internacional, Víctimas en el exterior)
		Reducir	El enlace de gestión documental del grupo Gestionara la recepción y custodia de las listas de asistencia físicas al finalizar las jornadas de atención a víctimas en el exterior. Como evidencia se crea un formato de entrega con las siguientes especificaciones (fecha, nombre de quien entrega y firma). Este archivo se almacenara en la oficina de la coordinadora de Grupo.	1 Archivo con las listas de asistencia de cada una de las jornadas de atención a víctimas en el exterior, de acuerdo a la programación del Grupo	01/06/2018	Enlaces SIG del GAVE


 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 6 de 19

4.1.3. Gestión De Información


	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001: 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 como consecuencia de: - Acciones involuntarias y/o deliberadas de usuario y/o - Vandalismo o hurto Activos críticos: GI-DES-001,GI-DES-002,GI-DES-003,GI-DES-004,GI-DES-005,GI-DES-006,GI-DES-007,GI-DES-008,GI-DES-009,GI-DES-010,GI-DES-011,GI-DES-012,GI-DES-013,GI-DES-014,GI-DES-015,GI-DES-017,GI-DES-018,GI-DES-019,GI-DES-020,GI-DES-021,GI-DES-022,GI-DES-023,GI-DES-024,GI-DES-025,GI-DES-026,GI-DES-027,GI-DES-028,GI-DES-029,GI-DES-030,GI-DES-031,GI-DES-032,GI-DES-033,GI-DES-034,GI-DES-035,GI-DES-036,GI-DES-037,GI-DES-038,GI-DES-039,GI-DES-040,GI-DES-041,GI-DES-042,GI-DES-043,GI-DES-044,GI-DES-045,GI-DES-046,GI-DES-047,GI-DES-048,GI-DES-049,GI-DES-050,GI-DES-051,GI-DES-052,GI-DES-053,GI-DOT-	Extrema	Reducir	Socializar mensualmente 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	Ocho (8) Boletines y/o Flash Informativos de Socialización relacionados con el aseguramiento de la información, durante el periodo de Mayo a Diciembre.	01/05/2018	Equipo de Seguridad y Riesgo informático - OTI
		Reducir	Formular la versión final del documento para realizar el monitoreo de capacidad disponible de almacenamiento, RAM y procesamiento de servidores y uso de canales de conectividad	Un (1) documento para realizar el monitoreo de capacidad disponible de almacenamiento, RAM y procesamiento de servidores y uso de canales de conectividad con fecha de entrega de Junio a Diciembre.	01/06/2018	Líder del equipo de Infraestructura - OTI; Equipo de Seguridad y Riesgo Informático; Enlace SIG_OTI
		Reducir	Formular el procedimiento o protocolo base de Gestión de cambios, en articulación con los procedimientos vigentes relacionados por tecnologías de la información.	Un (1) procedimiento o protocolo de Gestión de cambios con fecha de entrega de Junio a Diciembre de 2018.	01/06/2018	Equipo de Sistemas de Información - OTI; Equipo de Infraestructura OTI; Equipo de Seguridad y Riesgo informático - OTI; Enlace SIG
		Reducir	Formular el protocolo de borrado seguro, en articulación con los procedimientos vigentes relacionados por tecnologías de la información.	Un (1) protocolo de borrado seguro con fecha de entrega de Junio a Diciembre de 2018.	01/06/2018	Equipo de Dotación y soporte TI; Equipo de Seguridad y Riesgo Informático; Enlace SIG

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 7 de 19


Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
056,GI-SEG-071,GI-SEG-072,GI-DES-075,GI-DES-076,GI-DES-077. ACTIVOS SRNI - Activo 1 GI-AIDI-002 - Activo 2 GI-AIDI-003 - Activo 3 GI-AIDI-006 - Activo 4 GI-AIDI-043 - Activo 5 GI-AIDI-044 - Activo 6 GI-ANL		Reducir	Sensibilizar a los usuarios en el uso masivo de la herramienta tecnologica ONE DRIVE, en articulacion con el equipo de trabajo de uso y apropiación de la Oficina de Tecnologías de Información.	Cuatro (4) Sesiones de Socialización de la herramienta de almacenamiento one drive, a enlaces del SIG, durante el periodo de mayo a diciembre	01/05/2018	Equipo de Seguridad y Riesgo Informático
		Reducir	Generar el procedimiento de control de entregas de archivos planos o de información individualizada digital en medios magneticos, mediante claves de acceso para la visualización del dato.	1 procedimiento	01/08/2018	Instrumentalización de la Información
RSEG003:Pérdida de confidencialidad, integridad o disponibilidad ocasionada por la infiltración en el servidor , en el dispositivo de red y/o el sistema de información debido al acceso no autorizado como consecuencia de captura de credenciales transferidas en texto claro, durante el ingreso vía web. Activos: Servidores.	Moderada	Reducir	Actualizar la lista de verificación de Requisitos de Seguridad en la documentación de los sistemas de información críticos existentes y a los nuevos desarrollos, por parte del equipo de Sistemas de Información.	Actualizar el cumplimiento de la lista de verificación de Requisitos de Seguridad en la documentación de diez (10) sistemas de información críticos en un periodo de Junio a diciembre de 2018	01/06/2018	Equipo de Sistemas de Información - OTI; Equipo de Seguridad y Riesgo informático - OTI
		Reducir	Implementar y/o renovar certificados digitales en Sistemas de Información priorizados. Cómo evidencia se generan los nuevos certificados digitales.	Implementación y/o renovación de certificados digitales en tres (3) Sistemas de Información priorizados en un periodo de junio a diciembre de 2018	01/06/2018	Equipo de Sistemas de Información - OTI; Equipo de Infraestructura OTI; Equipo de Seguridad y Riesgo informático - OTI
		Reducir	Socializar mensualmente los productos presentados en el marco de los encuentros de enlaces SIG y/o los boletines o flash informativos que se	Ocho (8) Boletines y/o Flash Informativos de Socialización relacionados con el aseguramiento de la información, durante	01/05/2018	Equipo de Seguridad y Riesgo informático - OTI

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 8 de 19

	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
			generen en materia de seguridad de la información	el periodo de Mayo a Diciembre.		
RSEG007: Pérdida de disponibilidad y/o integridad en ambiente productivo en el sistema al presentarse errores durante la ejecución de modificaciones debido a la falta de definición, aplicación u omisión de alguna de las actividades del procedimiento de gestión de cambios. Activos : TOP 10 DE APLICATIVOS críticos.	Alta	Reducir	Formular el procedimiento o protocolo base de Gestión de cambios, en articulación con los procedimientos vigentes relacionados por tecnologías de la información.	Un (1) procedimiento o protocolo de Gestión de cambios con fecha de entrega de Junio a Diciembre de 2018.	01/06/2018	Equipo de Sistemas de Información - OTI; Equipo de Infraestructura OTI; Equipo de Seguridad y Riesgo informático - OTI; Enlace SIG
RSEG008: Pérdida de disponibilidad, integridad y/o confidencialidad en el sistema de información debido a ausencia o insuficiencia de copias de respaldo; o debido a vulnerabilidades no corregidas explotadas y/o falta de protección por código malicioso. Activos: Top 10 de aplicativos. Incluyendo el servidor Totoro.	Alta	Reducir	Actualizar el documento de generación de copias de respaldo de servidores de aplicación, base de datos y file servers	Un (1) documento actualizado para la generación de Copias de Respaldo durante el periodo de septiembre a Diciembre de 2018	01/09/2018	Equipo de Infraestructura - OTI
RSEG009: Pérdida de la confidencialidad de información física o digital debido a actividades de ingeniería social de un intruso que aproveche el desconocimiento de políticas, procedimientos y directrices de seguridad por parte de un colaborador, proveedor y/o	Alta	Reducir	Socializar mensualmente 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	Ocho (8) Boletines y/o Flash Informativos de Socialización relacionados con el aseguramiento de la información, durante el periodo de Mayo a Diciembre.	01/05/2018	Equipo de Seguridad y Riesgo informático - OTI
	Alta	Reducir	Reportar incidentes de seguridad, relacionados con ingeniería social, al CSIRT gobierno, con base en el procedimiento de	Por demanda, realizar reporte cada vez que se genere o se materialice un incidente de seguridad	01/06/2018	Gestión de Tecnologías de la Información


 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 9 de 19

	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
terceras partes. *Información			Gestión de incidentes de seguridad.	relacionado con ingeniería social		

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 10 de 19

4.1.4. Registro y Valoración


Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001*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. *ID DE LOS ACTIVOS ASOCIADOS: GR-LDR-003 GR-ARA-001 GR-ARA-002 GR-ARA-012 GR-CRN-004 GR-DEV-003 GR-DIG-010 GR-DIS-009 GR-DIS-010 GR-DIS-001 GR-DIS-004 GR-LDR-001 GR-DIG-001 GR-ARA-009 GR-TLI-005 GR-TLI-006 GR-TLI-009 GR-TLI-010 GR-TLI-011 GR-TLI-013 GR-TLI-014 GR-TLI-015 GR-GLO-001 GR-ARA-006 GR-VAL-004 GR-VAL-002 GR-VAL-007 GR-VAL-010 GR-VAL-031 GR-VAL-001 GR-VAL-017 GR-VAL-019 GR-VAL-020 GR-VAL-021 GR-VAL-030 GR-VAL-023 GR-VAL-034 GR-VAL-027 GR-VAL-028 GR-VAL-037 GR-VAL-005 GR-VAL-033 GR-EXC-001 GR-EXC-002 GR-EXC-005 GR-EXC-007 GR-TUT-001 GR-TUT-002 GR-REC-001 GR-REC-002 GR-REC-003 GR-REC-004 GR-REC-005 GR-	Alta	Reducir	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	3 boletines o flash informativos	01/06/2018	Grupo de capacitaciones

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 11 de 19


Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
REC-006 GR-REC-009 GR-REC-010 GR-NOV-001 GR-NOV-003 GR-NOV-004 GR-NOV-006 GR-NOV-007 GR-NOV-009 GR-NOV-010 GR-NOV-011 GR-NOV-012 GR-NOV-013 GR-TL2-001 GR-TL2-002 GR-TL2-003 GR-TL2-004 GR-TL2-005 GR-REG-001 GR-REG-002 GR-REG-003 GR-REG-004 GR-REG-005 GR-REG-006 GR-REG-007 GR-REG-008 GR-REG-0010 GR-VAL2-003 GR-VAL2-005 GR-VAL2-007		Transferir o Compartir	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.	1 Socialización	01/06/2018	Enlace SIG-OTI

4.1.5. Control Interno Disciplinario

Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001: 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 Activos críticos: CD-DIS-002 - CD-DIS-003, CD-DIS-004 , CD-DIS-005 , CD-DIS-006 .	Alta	Reducir	Solicitar a la OTI realizar un backup y capacitación respecto a cómo se debe guardar la información en ONE DRIVE (NUBE), a los funcionarios y contratistas del proceso, con el fin de blindar la información que se tiene de cada expediente digital, en caso de que haya una falla en los equipos o del ingreso de un virus que borre la información.	1 solicitud	1 de mayo de 2018	Coordinador Grupo de Control Interno Disciplinario
	Alta	Reducir	Solicitar a secretaria general espacio físico para el archivo de los	1 solicitud	1 de mayo de 2018	Coordinador Grupo de Control


 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 12 de 19

	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
			expedientes disciplinarios del grupo, para evitar la pérdida física de ellos			Interno Disciplinario


 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 13 de 19

4.1.6. Reparación Integral

Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
<p>RSEG001: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 como consecuencia de Vandalismo o hurto y/o acciones involuntarias y/o deliberadas del usuario. Activos Críticos Asociados: activos críticos asociados:</p> <p>DR-FRV-001; DR-FRV-002; DR-FRV-003; DR-FRV-004; DR-FRV-005; DR-FRV-006; DR-FRV-007; DR-FRV-008; DR-FRV-009; DR-FRV-010; DR-FRV-011; DR-FRV-012; DR-FRV-013; DR-FRV-017; DR-FRV-018; DR-FRV-020; DR-FRV-021; DR-FRV-022; DR-FRV-023; DR-FRV-024; DR-FRV-025; DR-FRV-026; DR-FRV-036; DR-FRV-038; DR-FRV-039; DR-FRV-040; DR-FRV-041; DR-FRV-042; DR-FRV-043; DR-GRR-001; DR-GRR-002; DR-GRR-003; DR-GRR-004; DR-GRR-005; DR-GRR-006; DR-GRR-007; DR-GRR-008; DR-GRR-009; DR-GRR-010; DR-GRR-012; DR-GRR-013; DR-GRR-014; DR-GRR-015; DR-SRC-001; DR-SRC-003; DR-SRC-004; DR-SRC-008; DR-SRC-009; DR-SRC-012; DR-SRC-013; DR-SRC-015; DR-SRC-016; DR-SRI-001; DR-SRI-002; DR-SRI-003; DR-SRI-004; DR-SRI-005; DR-SRI-006; DR-SRI-007; DR-SRI-008; DR-SRI-009; DR-SRI-010; DR-SRI-011; DR-SRI-012; DR-SRI-013; DR-SRI-014; DR-SRI-015; DR-SRI-016; DR-SRI-017; DR-SRI-018; DR-SRI-019; DR-SRI-020; DR-SRI-021; DR-SRI-022; DR-SRI-023; DR-SRI-024; DR-SRI-025; DR-SRI-026.</p>	Alta	Reducir	Generación de reportes de ingreso y uso del sistema de información de la Dirección de Reparación	Generar 8 reportes (uno mensual).	01/05/2018	Equipo Control y Seguimiento - Dirección de Reparación


 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 14 de 19

	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
	Alta	Reducir	Coordinar con la OTI la Restricción del uso de memorias o dispositivos de almacenamiento que permitan la extracción de información de la Dirección, como la infección de equipos afectando la información del Proceso.	100% de los equipos solicitados.	01/05/2018	Equipo Control y Seguimiento - Dirección de Reparación
	Alta	Reducir	Sensibilizar a los colaboradores para que hagan uso responsable en el acceso y manejo de la información de la Dirección de Reparación.	Realizar 8 procesos de sensibilización y socialización a funcionarios sobre uso de la información (uno mensual).	01/05/2018	Equipo Control y Seguimiento - Dirección de Reparación
	Alta	Reducir	Realizar revisión trimestral de los permisos de eliminación, modificación y/o consulta a los funcionarios del FRV en cuanto a los documentos de los expedientes digitales.	1 revisión trimestral.	01/05/2018	Responsable del Archivo físico y Digital.

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 15 de 19


4.1.7. Prevención De Hechos Victimizantes

Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001: 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. GP-PAE-001, GP-PAE-003, GP-PAE-004	Moderada	Reducir	Realizar socialización al interior del proceso de los temas de seguridad de la información y los posibles riesgos a los que se expone la información por conductas inadecuadas de los usuarios.	2 socializaciones	01/05/2018	Enlace SIG del proceso
		Reducir	Promover el uso de tecnologías (One drive) de Microsoft Office 365, para generar copia de respaldo de los archivos almacenados en los equipos de cómputo de los usuarios.	2 socializaciones	01/05/2018	Enlace SIG del proceso

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 16 de 19

4.1.8. Gestión Jurídica

	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001: 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 - 002, OJ - AAC - 003, OJ - AAC - 004, OJ - AAC - 005, OJ - AAC - 006, OJ - DFJ - 007, OJ - DFJ - 008, OJ - DFJ - 009, OJ - DFJ - 010, OJ - DFJ - 011, OJ - DFJ - 012, OJ - DFJ - 013)	Moderada	Reducir	Gestionar copia de respaldo y/o almacenamiento de todas las hojas de cálculo o archivos de Excel de la Oficina Asesora Jurídica en el mecanismo de almacenamiento que se defina en articulación con la Oficina de tecnologías de la información	1 gestión de copias de respaldo y/o almacenamiento	01/06/2018	Administrativos encargados de la Base de datos
		Reducir	Realizar un monitoreo de los permisos de acceso, modificación y eliminación que tienen las hojas de cálculo o archivos de Excel en el Servidor de la Unidad	trimestral	01/05/2018	Administrativos encargados de la Base de datos


 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 17 de 19

4.1.9. Gestión Para La Asistencia

Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001: 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. GA-BDD-007; SC-BDD-008; GA-BMT-011; GA-BSM-012	Alta	Evitar	La Subdirección de Asistencia y Atención Humanitaria, a través de la línea de acción Gestión Integral divulga a través de correo electrónico y/o reuniones de equipo las notas informativas que se generan de la Oficina de Tecnologías de la Información frente a tips de seguridad de la información, de esta actividad queda como registro correo electrónico o actas de reunión	1 actividad de divulgación de información cada dos meses	01/05/2018	Subdirector Técnico


4.1.10. Talento Humano

Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG008: Pérdida de disponibilidad, integridad y/o confidencialidad en el sistema de información debido a ausencia o insuficiencia de copias de respaldo; o debido a vulnerabilidades no corregidas explotadas y/o falta de protección por código malicioso. TH-VIA-027 / TH-NOM-029 / TH-HLF-031	Moderada	Reducir	Gestionar el respaldo de la información almacenada en equipos de cómputo asignados al usuario, teniendo en cuenta Onedrive o servidor de archivos Totoro.	100% de los funcionarios y contratistas del área conocen y aplican la herramienta OneDrive	01/05/2018	Enlace SIG
		Reducir	El enlace SIG gestionará con la OTI actividad de sensibilización con el personal del área sobre seguridad de la información	1 actividad de sensibilización	01/06/2018	Enlace SIG

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 18 de 19

Riesgo	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
<p>RSEG010 Pérdida en la integridad de la Imagen y reputación de la entidad o sanciones disciplinarias y/o penales por incumplimiento de la normatividad y regulaciones ocasionadas por la divulgación no autorizada o fuga de información o por el uso de software no legal o plagio; o por divulgación de las credenciales de los equipos de cómputo o aplicativos o incumplimiento de los términos por la pérdida o daño de la documentación o incumplimiento a los acuerdos de Nivel de Servicio.</p> <p>TH-SST-007 / TH-HLF-010 / TH-SST-012 / TH-SST-013 / TH-VIA-027 / TH-NOM-029 / TH-VIN-030 / TH-HLF-031</p>	Alta	Reducir	Gestionar el préstamo de un disco duro cifrado para transportar información sensible.	1 Disco duro cifrado.	01/06/2018	Gestión Interinstitucional
<p>RSEG010 Pérdida en la integridad de la Imagen y reputación de la entidad o sanciones disciplinarias y/o penales por incumplimiento de la normatividad y regulaciones ocasionadas por la divulgación no autorizada o fuga de información o por el uso de software no legal o plagio; o por divulgación de las credenciales de los equipos de cómputo o aplicativos o incumplimiento de los términos por la pérdida o daño de la documentación o incumplimiento a los acuerdos de Nivel de Servicio.</p> <p>TH-SST-007 / TH-HLF-010 / TH-SST-012 / TH-SST-013 / TH-VIA-027 / TH-NOM-029 / TH-VIN-030 / TH-HLF-031</p>		Reducir	Gestionar el respaldo de la información almacenada en equipos de cómputo asignados al usuario, teniendo en cuenta OneDrive o servidor de archivos Totoro	1 gestión de copias de respaldo y/o almacenamiento.	01/07/2018	Enlace SIG Y Oficina de Tecnología de la Información.

4.1.11. Participación y Visibilización de las Víctimas

 UNIDAD PARA LAS VÍCTIMAS	PLAN TRATAMIENTO RIESGOS SEGURIDAD DE LA INFORMACIÓN			
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	Código: 130,06,07-2	Versión: 1	Fecha: 18/06/2018	Página 19 de 19

	Riesgo Residual	PLAN DE RESPUESTA AL RIESGO (PROCESO)				
Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se debe llevar a cabo la acción)	Responsable (cargo)
RSEG001: Pérdida parcial o total de la confidencialidad, integridad y/o disponibilidad de las listas de asistencia, actas y archivos impresos y digitales que tiene a su cargo del Proceso de Participación. Activos Críticos: SP-AET-003 SP-AET-004 SP-AET-005	Alta	Reducir	Se realizará una capacitación con el acompañamiento de la Oficina de Tecnologías de la Información, para que los colaboradores del equipo de Participación sean concientizados del buen uso de los recursos para salvaguardar la información que tiene a disposición la entidad.	1 Capacitación	14/05/2018	Enlace Sig del Proceso
			Capacitar a los colaboradores del proceso de Participación sobre el uso de códigos de seguridad a los archivos	1 Capacitación	14/05/2018	Enlace Sig del Proceso

Anexo 1 Control de cambios

Versión	Fecha del cambio	Descripción de la modificación
1	18 de Junio 2018	Creación