El futuro es de todos

Unidad para la atención y reparación integral a las víctimas

Plan de tratamiento de riesgos de seguridad de la información 2019.

TABLA DE CONTENIDO

Contenido

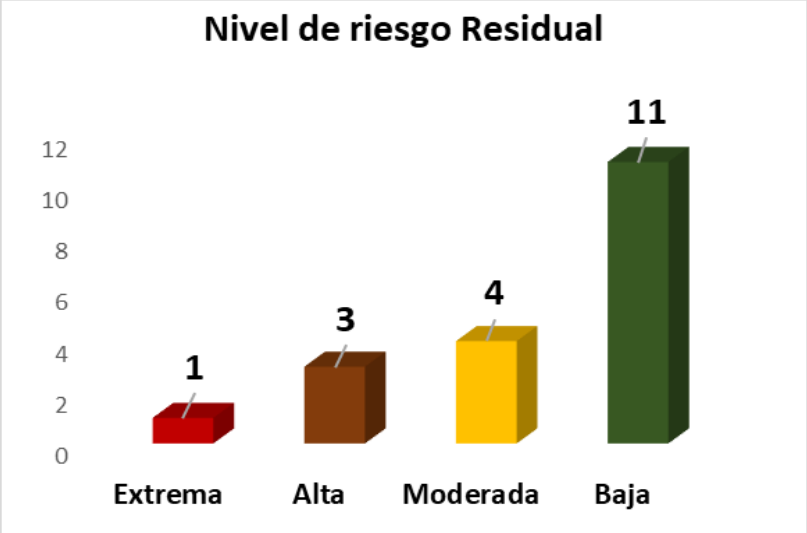
1. OBJETIVO

El objetivo del presente documento es consolidar los planes de tratamiento al riesgo generados en apoyo a la labor de la actividad de identificación de riesgos de seguridad de la información a los procesos con activos críticos definidos, seguido a esta gestión realizar el correspondiente seguimiento y verificación al cumplimiento de los planes de tratamiento al riego de seguridad de la información, en el marco de la metodología para la administración de riesgos definida por la Entidad.

2. ALCANCE

Los riesgos de seguridad de información actualmente identificados se encuentran asociados a los activos críticos1 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 definir 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 los riesgos según el nivel de riesgo residual:



Es importante mencionar que, según la metodología establecida en la Entidad los riesgos con nivel: moderado, alto y extremo, deben contar con su correspondiente plan de tratamiento al riesgo, sin embargo, se debe precisar que el proceso de Reparación Integral, de manera autónoma, generó un plan de tratamiento para un riesgo con nivel bajo, el cual se incluye en el presente documento.

[1] Se considera activo crítico cuando 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.

3. ACTIVIDADES

A continuación, se presentan los planes de tratamiento de riesgos de seguridad de la información definidos por cada proceso de la Entidad:

3.1. Registro y valoración

IDENTIFICACION	IDENTIFICACION					VALORACION			TRATAMIENTO						
						RIESGO RESIDUAL			PLAN DE TRATAMIENTO AL RIESGO						ACCION SI EL RIESGO SE MATERIALIZA
Proceso o DT	**Actividad**	**Causas/ Vulnerabilidades**	**Riesgo**	**Consecuencias/ Amenazas**	**Tipo de Riesgo**	**Probabilidad**	**Impacto**	**Zona de Riesgo**	**Medida de Tratamiento**	**Acción**	**Meta** (cantidad y periodicidad)	**Fecha de Inicio** (A partir de esa fecha se debe llevar a	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	
REGISTRO Y VALORACION	Definir los medios, instrumentos, mecanismos mediante los cuales se tomará la declaración para decidir sobre la inclusión o no en el Registro Único de Víctimas de las personas que declaran por los hechos victimizantes estipulados en la Ley 1448 de 2011, resolver los recursos de la vía administrativa y atender a las solicitudes de ingreso por vía judicial, actualizar la información en el RUV con el fin que las victimas tengan acceso a las medidas de asistencia, atención y reparación establecidos en la ley.	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. GR-ARA-002; GR-DIS-004; GR-DIS-009; GR-DIS-012; GR-DIS-013; GR-DIS-015; GR-EXC-026; GR-EXC-001; GR-EXC-005; GR-EXC-007; GR-EXC-008; GR-EXC-009; GR-EXC-010; GR-EXC-011; GR-EXC-012; GR-EXC-013; GR-EXC-014; GR-EXC-015; GR-EXC-016; GR-EXC-017;GR-EXC-018; GR-EXC-019; GR-IMG-001; GR-IMG-002;GR-IMG-003; GR-IMG-004; GR-IMG-005; GR-LDR-002;GR-NOV-006; GR-NOV-007; GR-NOV-009; GR-NOV-010; GR-NOV-013; GR-NOV-014; GR-NOV-015; GR-NOV-016; GR-REC-004; GR-REC-005; GR-REC-006; GR-REC-009; GR-REC-010; GR-NOV-017; GR-NOV-019; GR-REG-001; GR-REG-002; GR-REG-006; GR-REG-007; GR-REG-008; GR-REG-010; GR-REG-017; GR-REG-018; GR-REG-019; GR-TL2-001; GR-TL2-003; GR-TL2-005; GR-TLI-005; GR-TLI-009; GR-TLI-010; GR-TLI-011; GR-TLI-014; GR-TUT-001; GR-TUT-002; GR-VAL-002; GR-VAL-005; GR-VAL-007; GR-VAL-017; GR-VAL-020; GR-VAL-020; GR-VAL-023; GR-VAL-027; GR-VAL-028; GR-VAL-031; GR-VAL-034; GR-VAL2-010; GR-VAL2-011; GR-DIS-014; GR-NOV-001; GR-NOV-003; GR-NOV-011; GR-NOV-012; GR-VAL-001; GR-VAL-021; GR-VAL-030; GR-ARA-001; GR-NOV-018.	Divulgación de datos sensibles. Corrupción de datos Datos provenientes de fuentes no confiables Error en el uso de los datos. Manipulación del Software Acciones no autorizadas Daños físicos	Seguridad de la información y seguridad digital	3	2	Moderada	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.	1 socializacion mensual	01/07/2019	3 meses	Enlace SIG en articulación con la OTI	Establecer en el menor tiempo posible una reunión con la OTI y los líderes de los procedimientos para establecer una estrategia que resuelva la incidencia presentada.
		Ausencia de mecanismos de monitoreo							Evitar	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 socializacion mensual	01/07/2019	3 meses	Enlace SIG en articulación con la OTI	
		Descarga y uso no controlados de software													
		Ausencia de copias de respaldo													

3.2. Reparación Integral

							TRATAMIENTO						
				RIESGO RESIDUAL			PLAN DE TRATAMIENTO AL RIESGO						
Actividad	**Causas/ Vulnerabilidades**	**Riesgo**	**Consecuencias/ Amenazas**	**Probabilidad**	**Impacto**	**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)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	**ACCIÓN SI EL RIESGO SE MATERIALIZA**
Transversal al Proceso Reparación Integral.	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 registrada en documento físico o digital. *Activos críticos asociados.	* Pérdida Información sensible. * Parálisis en los procesos. * Modificación por error en Uso. * Modificación por corrupción de datos. * Divulgación accidental. * Pérdida - destrucción por manipulación de software. * Pérdida - destrucción por hurto de	2	2	Baja	Reducir	Sensibilizar a los colaboradores para que hagan uso responsable en el acceso y manejo de la información de la Dirección de Reparación.	Realizar 5 procesos de sensibilización y socialización a funcionarios sobre uso de la información (Por lo menos uno mensual).	01/07/2019	5 meses	Equipo Control y Seguimiento - Dirección de Reparación	Verificar las copias de seguridad con los que cuenta la Unidad Para las Víctimas (digitales y físicos) y realizar la reconstrucción de la información faltante.
	Acciones involuntarias y/o deliberadas de usuario por ausencia o insuficiencia en la gestión de eventos de monitoreo o por almacenamiento de información						Reducir	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.	01/07/2019	5 meses	Equipo Control y Seguimiento - Dirección de Reparación	
	Acceso no controlado a información sensible / confidencial.												

3.3. Gestión Jurídica

							TRATAMIENTO						
				RIESGO			PLAN DE TRATAMIENTO AL RIESGO						ACCION SI EL RIESGO SE MATERIALIZA
Actividad	**Causas/ Vulnerabilidades**	**Riesgo**	**Consecuencias/ Amenazas**	**Probabilidad**	**Impacto**	**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)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	
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 FRV	Almacenamiento de informacion de los procesos en bases planas.	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 - AA- 017,OJ - AA- 018,OJ - AA- 019,OJ - AA- 020,OJ - DF - 008,OJ - DF - 009,OJ - DF - 010, OJ - DF - 011,OJ - DF - 012,OJ-OAJ-001,OJ-OAJ-002,OJ-OAJ-003,OJ-OAJ-004.**	Perdida-Destrucción debido a Mal funcionamiento del Software. Perdida y/o destrucción debido a manipulación del software. Interrupción debido a la saturación del sistema de información. Divulgación de la información debido a Copia fraudulenta del Software. Modificación de la información debido a procesamiento ilegal de los datos	2	3	**Moderada**	Reducir	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	Diario	01/08/2019	6 meses	Jefe de la Oficina Asesora Juridica	Gestionar con el operador y/o operadores de manera manual el personal que se desvincula, para validar realizar la inactivación oportuna de credenciales de acceso a sistemas de información.
	Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.												
	Acceso no controlado a información sensible / confidencial.												

3.4. Gestión de talento humano

							TRATAMIENTO						
				RIESGO			PLAN DE TRATAMIENTO AL RIESGO						ACCION SI EL RIESGO SE MATERIALIZA
Actividad	Causas/ Vulnerabilidades	Riesgo	Consecuencias/ Amenazas	Probabilidad	Impacto	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)	Duración (meses durante los cuales se va a cumplir la meta)	Responsable (cargo)	
Administrar historias laborales y SIGEP	* Insuficiencia de controles de acceso a las instalaciones * Ausencia de mecanismos de digitalización o herramientas de sistematización que brinden respaldo a la información * Insuficiente personal capacitado y con responsabilidades específicas en la custodia de expedientes	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. (ID TH-HLF-010, TH-VIN-030)	* Divulgación accidental de la información por abuso de derechos * Pérdida o destrucción de la información por daños en los equipos o medios de conservación. * Interrupción del servicio por incumplimiento en la disponibilidad del personal * Pérdida o destrucción de la información por hurto de medios o documentos * Modificación de la información por datos provenientes de fuentes no confiables *Modificación de información por Falsificación de derechos * Retraso en los procesos * Certificación de información errada * Investigaciones disciplinarias * Pérdida de información sensible	1	4	Alta	Reducir	Implementar y difundir instrumentos de gestión documental para el control de historias laborales	1 Actividad de implementación y difusión de instrumentos de gestión documental para historias laborales	01/08/2019	5 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.
							Reducir	Implementar herramientas tecnológicas que fortalezcan la administración y control de historias laborales articuladas con los lineamientos técnicos impartidos por la OTI	1 Herramienta tecnológica para la administración y control de historias laborales implementada	01/07/2019	12 meses	Coordinador Talento Humano	
							Reducir	Retomar administración de historias laborales organizando área de archivo exclusivo y restringido	1 Área de archivo de historias laborales organizado y controlado por Talento Humano	01/08/2019	5 meses	Coordinador Talento Humano	
Administrar la nómina, seguridad social y prestaciones de los funcionarios	* Fallas recurrentes e insuficiente capacidad funcional y de cumplimiento legal en la plataforma utilizada sin soporte tecnológico adecuado * Ausencia o insuficiencia de control de cambios en la configuración * Dependencia de proveedores.	Pérdida total o parcial de la confidencialidad y/o integridad de la información registrada en sistema de información de nómina debido al mal funcionamiento y/o manipulación de manera accidental o deliberada por usuarios internos o externos. (ID TH-NOM-029)	* Divulgación de información por uso no autorizado del equipo * Interrupción del servicio por mal funcionamiento de software * Modificación de información por manipulación con software * Modificación accidental de informaicón por corrupción de datos * Divulgación de información por abuso de derechos de usuarios externos * Modificación de información por expionaje remoto	3	4	Extrema	Reducir	Implementar herramientas tecnológicas que fortalezcan el trámite y control de la nómina, seguridad social y prestaciones articulada con los lineamientos técnicos impartidos por la OTI	1 Herramienta tecnológica para la administración y de nómina implementada	01/07/2019	12	Coordinador Talento Humano	Realizar verificación exhaustiva de la trazabilidad y control de los registros del aplicativo y de confirmarse la materialización, poner en conocimiento de las instancias competentes.

3.5. Gestión para la asistencia

							TRATAMIENTO						
				RIESGO			PLAN DE TRATAMIENTO AL RIESGO						
Actividad	**Causas/ Vulnerabilidades**	**Riesgo**	**Consecuencias/ Amenazas**	**Probabilidad**	**Impacto**	**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)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	**ACCION SI EL RIESGO SE MATERIALIZA**
Analizar, tramitar las solicitudes y realizar la colocación de recursos a los registros viables por concepto de Atención Humanitaria y Ayuda Humanitaria.	Ausencia o insuficiencia de procedimientos de Monitoreo de los recursos de procesamiento de información.	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	* Legales * Credibilidad e Imagen • Perdida-Destrucción debido a inundación. • Interrupción debido a la saturación del sistema de información • Perdida-Destrucción debido a Manipulación Software	1	4	Alta	Evitar	Cada vez que se idenfifica la desvinculación de las personas que hacen parte de la operación relacionada con la prestación de los servicios del proceso, se realiza la inactivación oportuna de credenciales de acceso a sistemas de información a través de la documentación establecida para tal fin.	A necesidad	Julio de 2019	6 meses	Beatriz Carmenza Ochoa	La Subdirección de Asistencia y Atención Humanitaria a través de la línea de acción administración y gestión de requerimientos técnicos, 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.
	Acceso no controlado a información sensible / confidencial..												

3.6. Gestión de Información

						TRATAMIENTO						
			RIESGO RESIDUAL			PLAN DE TRATAMIENTO AL RIESGO						ACCION SI EL RIESGO SE MATERIALIZA
Actividad	**Causas/ Vulnerabilidades**	**Riesgo**	**Probabilidad**	**Impacto**	**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)	**Duración** (meses durante los cuales se va a cumplir la meta)	**Responsable** (cargo)	
-Desarrollar nuevas aplicaciones y sistemas de información (Sistemas de información) '-Soportar sistemas de información y aplicaciones -Gestionar las actividades derivadas de la implementación del subsistema de gestión de seguridad de la información (Seguridad de la Información)	Ausencia o insuficiencia de procedimientos de Monitoreo de los recursos de procesamiento de información.	Indisponibilidad, 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-013,TI-SIF-014,TI-SIF-015,TI-SIF-016,TI-SIF-017,TI-SIF-018,TI-SIF-019,TI-SIF-020,TI-SIF-021,TI-SIF-022,TI-SIF-023,TI-SIF-024,TI-SIF-025,TI-SIF-026,TI-SIF-027,TI-SIF-028,TI-SIF-029,TI-SIF-032,TI-SIF-034,TI-SIF-042,TI-SIF-043,TI-SIF-044,TI-SIF-046,TI-SIF-048,TI-SIF-049,TI-SIF-064,TI-SIF-065,TI-SIF-066,TI-SIF-067,TI-SIF-068	1	4	Alta	Reducir	Identificar los controles de seguridad relacionados con el ciclo de vida de la gestión de usuarios en sistemas de información e incluir estos controles en el procedimiento actual.	1 Documento con la identificación de controles, y actualización del procedimiento anual si aplica	01/07/2019	6	Lider de seguridad de la Información lider de sistemas de información	Realizar la investigación que permita diagnosticar la causa y tomar acción inmediata técnica, judicial o administrativa para corregir la situación
	Falla, daño o degradación de equipos.					Reducir	Diseñar e implementar la estrategia para la evaluación de la aplicación de las políticas de seguridad de la información	1 Estrategia para aplicar politica de seguridad, anual	01/07/2019	12	Lider de gobierno TI Lider de seguridad de la Información	
	Acceso no controlado a información sensible / confidencial.											
	Debilidades de los sistemas de información frente a requisitos de seguridad y privacidad de la información											
	Desarticulación respecto a tareas, actividades y desarrollos tecnológicos en el marco de la interoperabilidad con las dependencias que desarrollan sistemas de información											

El futuro es de todos | Unidad para la atención y reparación integral a las víctimas

Actividad	Causas/ Vulnerabilidades	Riesgo	RIESGO RESIDUAL			TRATAMIENTO						ACCION SI EL RIESGO SE MATERIALIZA
						PLAN DE TRATAMIENTO AL RIESGO						
			Probab	Impacto	Zona de	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de Inicio (A partir de esa fecha se	Duración (meses durante los cuales se va	Responsable (cargo)	
-Desarrollar nuevas aplicaciones y sistemas de información -Soportar sistemas de información y aplicaciones -Realizar soporte técnico a la infraestructura tecnológica -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 -Gestionar la solicitud de dotación tecnológica -Gestionar la infraestructura tecnológica asociada a los servicios de: buzones de correo institucional, acceso a servidores y bases de datos, telefonía IP. (Servicios tecnológicos) -Gestionar las actividades derivadas de la implementación del subsistema de gestión de seguridad de la información	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-002, TI-ARH-003, TI-ARH-005, TI-ARH-007, TI-ARH-008, TI-ARH-010	1	3	Moderada	Reducir	Generar, oficializar y ejecutar el plan de capacitación, sensibilización y comunicación de seguridad de la información con alcance central y territorial.	Plan de sensibilizqción aprobado por la jefatura OTI ejecutado anual	01/07/2019	6	Lider seguridad de la información Lider uso y apropiación	Realizar la investigación que permita diagnosticar la causa y tomar acción inmediata técnica, judicial o administrativa para corregir la situación
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los empleados y/o terceras partes.					Reducir	Realizar un ejercicio de ingeniería social que a través de la modalidad de phishing controlado sensibilice a los usuarios de la Entidad	1 Ejercicio de ingenieria social controlado anual	01/07/2019	6	Lider seguridad de la información Lider uso y apropiación	
	Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.					Reducir	Actualizar el procedimiento de creación de usuarios incluyendo la gestión de talento humano, contratos, operadores y administradores funcionales para la validación de la vigencia del usuario según la modalidad de contratación	1 procedimiento actualizado	01/07/2019	6	lider de seguridad de la información Lider de sistemas de información Lider de infraestructura	
	Acceso no controlado a información sensible / confidencial.											
	Ausencia o insuficiencia de controles de acceso a las instalaciones.											

						TRATAMIENTO						
Actividad	Causas/ Vulnerabilidades	Riesgo	RIESGO RESIDUAL			PLAN DE TRATAMIENTO AL RIESGO						ACCION SI EL RIESGO SE MATERIALIZA
			Probabilidad	Impacto	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)	Duración (meses durante los cuales se va a cumplir la meta)	Responsable (cargo)	
-Desarrollar nuevas aplicaciones y sistemas de información -Soportar sistemas de información y aplicaciones -Realizar soporte técnico a la infraestructura tecnológica -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 -Gestionar la solicitud de dotación tecnológica -Gestionar la infraestructura tecnológica asociada a los servicios de: buzones de correo institucional, acceso a servidores y bases de datos, telefonía IP. (Servicios tecnológicos) -Gestionar las actividades derivadas de la implementación del subsistema de gestión de seguridad de la información	Ausencia o insuficiencia de copias de respaldo.	Divulgación, modificación y/o destrucción de manera accidental y/o deliberada de la información de gestión del proceso y/o de los procesos de apoyo, que es considerada critica para la operación. TI-SEG-009, TI-SEG-010, TI-SEG-013, TI-SEG-036	1	3	Moderada	Reducir	Gestionar con el apoyo de los restantes procesos el análisis de impacto de operación con base en los activos criticos priorizados en el marco de subsistema de gestión de seguridad de información	1 Documento con el análisis de impacto de operación con base en activos criticos priorizados, anual	01/07/2019	6	Lider de seguridad de la Información enlace SIG	Realizar la investigación que permita diagnosticar la causa y tomar acción inmediata técnica, judicial o administrativa para corregir la situación
	Ausencia o insuficiencia de procedimientos para el manejo información clasificada.					Reducir	Realizar un seguimiento periodico por parte del equipo de seguridad y privacidad, a los reportes de disponibilidad de centro de datos y conectividad a nivel nacional	1 documento con el resultado semestral del seguimiento a centro de datos y conectividad, anual	01/07/2019	6	Lider de seguridad de la Información Lider de servicios tecnológicos Lider de infraestructura	

DOCUMENTO DE REFERENCIA

1. Metodología administración de riesgos 2019
2. Formato Levantamiento Mapa de Riesgos 2019
3. Inventario de activos de información

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	Julio 2019	Creación
2	Agosto 2019	Retroalimentación
3	Agosto 2019	Versión 1.0

Proyectó	Marcela Rocio Torres	Marcela Rocio Torres S.
Revisó	Joaquin Rojas Palomino	
Aprobó 20/08/2019	Martin Cubides Rojas	