GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

IDENTIFICACIÓN								CALIFICACIÓN				VALORACIÓN								PLAN DE TRATAMIENTO				
COMPONENTE O/O IOC	TIPO DE PROCESO	PROCESO	OBJETIVO DEL PROCESO	RIESGO	CAUSAS O EVENTOS	TIPO DE RIESGO	CONSECUENCIAS (RELACIONADAS DEL EVENTO)	PROBABILIDAD ESCALA ALTA (0.8 - 1.0) MEDIA (0.4 - 0.6) BAJA (0.0 - 0.2) Probabilidad = n	IMPACTO ESCALA CATASTRÓFICO (1.0) MAYOR (0.8) MODERADO (0.6) MENOR (0.4) LEVE (0.2) Impacto = n	EVALUACIÓN DEL RIESGO INHERENTE (Probabilidad x Impacto)	NIVEL DE RIESGO INHERENTE (BAJO, MODERADO, ALTO, EXTREMO)	CONTROLES EXISTENTES DE ESTABLECER LOS CONTROLES EXISTENTES	CANT. DE CONTROLES EXISTENTES (1 = Ninguno, 2 = Uno, 3 = Dos, 4 = Tres o más)	TIPO DE CONTROL 1= INDIRECTIVO 2= CORRECTIVO 3= PREVENTIVO	FRECUENCIA DEL CONTROL 1= OCASIONAL 2= FREQUENTE 3= PERMANENTE	PRODUCTO (TIPO DE CONTROL Y PERIODICIDAD DEL CONTROL)	EFICACIA DEL CONTROL	EVALUACIÓN DEL CONTROL (Valor Eficacia del Control x Producto)	NIVEL DE RIESGO RESIDUAL ALTO MODERADO BAJO	OPCIÓN DE TRATAMIENTO (Evitar, Reducir/Mitigar, Compartir/Transferir, Aceptar)	ACCIONES (Actividad a ejecutar para materializar la opción de tratamiento del riesgo, que permita el cumplimiento de la meta de control, Tipo)	RESPONSABLE (Área responsable de ejecutar)	CRONOGRAMA O/O PLAN DE ACCIÓN FECHA INICIO (dd/mm/aaaa)	FECHA FIN (dd/mm/aaaa)
Sistema de Gestión de Seguridad de Información (SGSI)	Evaluación_y_mejora		Evaluar el Sistema de Control Interno de la Unidad Nacional de Protección a través de Auditorías Seguimientos y Evaluaciones Independientes, y apoyar los demás sistemas de gestión implementados en la Entidad, que permita el mejoramiento continuo de la eficacia, eficiencia y efectividad de los procesos de la Entidad	**Posibilidad de comprometer la Integridad de la información institucional debido a fallas técnicas y operativas en el proceso**	* Tecnología| Mantenimiento insuficiente - 2 * Tecnología| Instalaciones de maquinarias - 1 * Tecnología| Ataques cibernéticos - 2 * Tecnología| Software malicioso - 2 * Personal| Inadecuada manejo de la información causada por una indebida manipulación de los sucesivos - 1 * Tecnología| Vulnerabilidades en la información - 1 * Tecnología| Desactualización en la información - 1 * Personal| Errores humanos - 3 * Personal| Desconocimiento de los usuarios en el manejo de las aplicaciones, sistemas de información y herramientas - 1 * Personal| Falta de planes de contingencia en Seguridad de la información - 1 * Personal| Falta de mecanismos de control de acceso físico a los activos de información - 1 * Personal| Falta de equipos - 1 * Personal| Falta de divulgación de las políticas y procedimientos propios del proceso - 1 * Tecnología| Insuficientes requerimientos de monitoreo de los servicios de red - 1 * Personal| Falta de socialización a todos los colaboradores sobre las buenas prácticas en la información en los diferentes repositorios institucionales asignados por la entidad - 1 * Tecnología| Inadecuada asignación de derechos de acceso a los repositorios institucionales - 1 * Personal| Desconocimiento en manejo adecuado de bases de datos institucionales - 1	Seguridad Digital	* Inconsistencias en la validación de la información preparatoria - 1 * Falsa información suministrada de los sistemas - 1 * Inadecuada toma de decisiones - 1 * Pérdida reputacional - 1 * Incumplimiento normativo - 1 * Procesos administrativos y/o judiciales - 1	2	6	12	MODERADO	1. Políticas de Seguridad Seguridad de la información Roles y Responsabilidades 2. Tareas y condiciones del empleo Durante la ejecución del empleo 3. Gestión de activos 3.1 Clasificación de la información 3.2 Transferencia de medios de soportes físicos 3.3 Mantenimiento de equipos 3.4 Procedimientos de operación documentados 3.5 Registros y seguimiento 3.6 Transferencia de información 3.7. Mensajes electrónicos	11	4	3	12	4	ALTO	BAJO	Mitigar el Riesgo	**1> Proponer acciones para mitigar los riesgos de seguridad digital identificados que son significativos, en cuanto a que son desproporcionadas, excesivas y complejas.** 2> Cumplir con los formatos, registros y procedimientos establecidos para realizar las acciones que se vienen de cumplimiento a las normas de auditorías de Control Interno. **3> Realizar seguimiento a los puntos de control establecidos en la matriz de riesgos institucional para una sola vez de los procedimientos verificando la eficiencia y no de eficiencia.** **4> Generar acciones de mejora cuando se evidenciar la inactividad y ausencia completa de los archivos de información, realizando check list, capacitación proceso, entre otros.**	Personas designadas en la Oficina de Control Interno		
Sistema de Gestión de Seguridad de Información (SGSI)	Evaluación_y_mejora		Evaluar el Sistema de Control Interno de la Unidad Nacional de Protección a través de Auditorías Seguimientos y Evaluaciones Independientes, y apoyar los demás sistemas de gestión implementados en la Entidad, que permita el mejoramiento continuo de la eficacia, eficiencia y efectividad de los procesos de la Entidad	**Posibilidad de comprometer la Integridad de la información institucional debido a fallas técnicas y operativas en el proceso**	* Personas| Desconocimiento en manejo de las aplicaciones, sistemas de información y herramientas - 1 * Personas| Falta de capacitación en los usuarios en el manejo de las aplicaciones, sistemas de información y herramientas - 1 * Personas| Desconocimiento a falta de capacitación en seguridad de la información - 1 * Personas| Falsas de capacitación de los usuarios de acuerdo con su rol - 1 * Personas| Falta de divulgación de las políticas, normas y procedimientos de seguridad de la información - 1 * Personas| Falta de asignación de los derechos de acceso al activo de información con los el funcionario asumiría de rol a su vez en la organización - 1 Inadecuada asignación de derechos de acceso a los repositorios institucionales - 1 * Personas| Falta de socialización a todos los colaboradores sobre las buenas prácticas en el almacenamiento de información en redes internas de acceso institucionales - 1 Facilidad de dar acceso público a la información - 1 Facilidad de dar acceso público a la información contenida en los repositorios institucionales - 1 Facilidad de extravío, pérdida, deterioro o daño del medios de almacenamiento - 1	Seguridad Digital	Desperfecto de la Seguridad de la Información	2	6	12	MODERADO	1. Políticas de Seguridad Seguridad de la información Roles y Responsabilidades 2. Tareas y condiciones del empleo Durante la ejecución del empleo 3. Gestión de activos 3.1 Clasificación de la información 3.2 Transferencia de medios de soportes físicos 3.3 Mantenimiento de equipos 3.4 Procedimientos de operación documentados 3.5 Registros y seguimiento 3.6 Transferencia de información 3.7. Mensajes electrónicos	14	4	2	8	3	MEDIO	BAJO	Mitigar el Riesgo	**1> Identificar y prevenir la divulgación de la información no autorizada.** **2> Restringir el acceso a los datos más valiosos** **3> Realizar auditorías sugirientes periódicas. Los controles establecidos** **4> Educar y enfocar los controles creados**	Planeación Responsables asignados por el área de tecnología		
Sistema de Gestión de Seguridad de Información (SGSI)	Evaluación_y_mejora		Evaluar el Sistema de Control Interno de la Unidad Nacional de Protección a través de Auditorías Seguimientos y Evaluaciones Independientes, y apoyar los demás sistemas de gestión implementados en la Entidad, que permita el mejoramiento continuo de la eficacia, eficiencia y efectividad de los procesos de la Entidad	**Posibilidad de comprometer la disponibilidad por dependencia (social y tecnológica) de los procesos de servicios TIC**	* Personas| Falta de capacitación en los usuarios de acuerdo con su rol - 1 * Personas| Falta de divulgación de las políticas, normas y procedimientos de seguridad de la información - 1 * Personas| Desconocimiento a falta de capacitación en seguridad de la información - 1 * Personas| Falta de divulgación de las políticas y procedimientos propios del proceso - 1 * Personas| Falta de socialización a todos los colaboradores sobre las buenas prácticas en el almacenamiento de información en redes internas de acceso institucionales - 1 Facilidad de dar acceso público a la información - 1 Facilidad de dar acceso público a la información contenida en los repositorios institucionales - 1 Facilidad de extravío, pérdida, deterioro o daño del medios de almacenamiento - 1	Seguridad Digital	Incumplimientos legales	3	9	27	ALTO	1. Políticas de Seguridad Seguridad de la información Roles y Responsabilidades 2. Tareas y condiciones del empleo Durante la ejecución del empleo 3. Gestión de activos 3.1 Clasificación de la información 3.2 Transferencia de medios de soportes físicos 3.3 Mantenimiento de equipos 3.4 Procedimientos de operación documentados 3.5 Registros y seguimiento 3.6 Transferencia de información 3.7. Mensajes electrónicos 3.8. Acuerdos de confidencialidad y/o de confidencialidad	13	4	3	12	4	ALTO	BAJO	Mitigar el Riesgo	**1> Planificar periódicamente copias de seguridad para garantiza la conservación y resguardo de la información institucional.** **2> Realizar copias de seguridad a los activos digitales de gestión y control de la entidad** **3> Realizar mantenimiento periódicos para garantizar la realización de las copias de los archivos digitales y la conservación y resguardo de los archivos digitales** **4> Generar oportunidades de mejora para las actividades identificadas en el desarrollo del proceso**	Planeación Responsables asignados por el área de tecnología		
Sistema de Gestión de Seguridad de Información (SGSI)	Evaluación_y_mejora		Evaluar el Sistema de Control Interno de la Unidad Nacional de Protección a través de Auditorías Seguimientos y Evaluaciones Independientes, y apoyar los demás sistemas de gestión implementados en la Entidad, que permita el mejoramiento continuo de la eficacia, eficiencia y efectividad de los procesos de la Entidad	**Posibilidad de no atender los requisitos de automatización de procesos de la entidad, que afecte la capacidad tecnica de los procesos adoptados.**	* Tecnología| Inconsistencias con los diseños del código fuente de las aplicativos, falta conocimiento de los mismos, o poca centralidad del negocio nuevamente en los diferentes grupos constituyentes que poseen el desarrollo y mantenimiento por falta de personal - 1 * Tecnología| Algunos sistemas Tic que soportan la operación de la entidad son especializados por ser sistemas no suministrados para atendimiento adecuadamente por el mercado - 1 * Tecnología| Contratación de productos TIC con especificaciones generales frente a las necesidades puntuales de la entidad, evidenciada en el momento de entrega de los productos - 1 * Personal| Falta claridad en la definición de requerimientos funcionales, los cuales no evidencian en el momento de entrega de los productos - 1 * Personal| Implementación de soluciones tecnológicas sin la validación y aceptación de los usuarios de la entidad - 1 * Personal| Desconocimiento de la normatividad en los políticas de seguridad y privacidad de la información - 1	Seguridad Digital	Incumplimientos legales	3	9	27	ALTO	1. Políticas de Seguridad Seguridad de la información Roles y Responsabilidades 2. Tareas y condiciones del empleo Durante la ejecución del empleo 3. Transferencia de medios de soportes físicos 3.7. Control de acceso a sistemas y aplicaciones 3. Restricción de acceso a la información 3. Procedimientos de operación documentados 3.5 Registros y seguimiento 3. Transferencia de información 3. Acuerdos de confidencialidad y/o de confidencialidad	12	2	2	4	2	BAJO	MODERADO	Mitigar el Riesgo	**1> Planificar el objetivo y alcance que se quiere lograr para automatizar los procesos de la entidad** **2> Identificar y priorizar las áreas para automatizar de acuerdo a los procesos que requieren de una eficiencia y seguridad mayor de la entidad** **3> Realizar supervisión y revisión del curso del proceso de automatización para garantizar que se ajuste a la caracterización de los procesos de acuerdo a la necesidad** **4> Generar oportunidades de mejora a las debilidades encontradas para mitigar los riesgos en el desarrollo del proyecto y que garantice no interrumpir/evitar fuera el flujo**	Planeación, Área de Tecnología y Líderes de los Procesos de la entidad		
Sistema de Gestión de Seguridad de Información (SGSI)			Evaluar el Sistema de Control Interno de la Unidad Nacional de Protección a través de Auditorías Seguimientos y Evaluaciones Independientes, y apoyar los demás sistemas de gestión implementados en la Entidad, que permita el mejoramiento continuo de la eficacia, eficiencia y efectividad de los procesos de la Entidad	**Posibilidad de tener Sistemas de información desactualizados, que afecte debido a la Disponibilidad en continuidad a los contratos de soporte y mantenimiento**	* Tecnología| El fabricante del sistema de información está continuando para mantener los productos del Estado - 1 * Tecnología| Falta de recursos para dar continuidad a contratos de soporte y mantenimiento - 1 * Financieros| No contar con recursos económicos para realizar procesos/inversión de los sistemas de información - 1	Seguridad Digital	Incumplimientos legales	2	6	12	MODERADO	* Verificación de la seguridad de la información * Verificación de la continuidad de la seguridad de la información * Implementación de la continuidad de la seguridad de la información	4	2	2	4	2	BAJO	BAJO	Mitigar el Riesgo	**1> Planificar la contratación de un Software Integral de Seguridad de la Información** **2> Realizar mantenimiento periódicos anos componentes de la entidad para garantizar el impacto y alcance del mismo** **3> Realizar mantenimiento periódico desde la supervisión que garantice mantener la gestión y avance del proyecto** **4> Realizar mesas de trabajo cuando que puedan evitar la ejecución del proyecto, para generar soluciones a corporatas inmediatas que garanticen la continuidad y culminación del proyecto**	Dirección Planeación Secretaria General Líderes de los Procesos de la entidad		
Sistema de Gestión de Seguridad de Información (SGSI)			Evaluar el Sistema de Control Interno de la Unidad Nacional de Protección a través de Auditorías Seguimientos y Evaluaciones Independientes, y apoyar los demás sistemas de gestión implementados en la Entidad, que permita el mejoramiento continuo de la eficacia, eficiencia y efectividad de los procesos de la Entidad	**Posibilidad de tener alteraciones de información que afecte la Disponibilidad de la información por errores humanos**	* Personal| Desconocimiento/poca/incumplimiento de las políticas de seguridad y privacidad de la información.	Seguridad Digital	Incumplimientos legales	1	9	9	BAJO	1. Políticas de Seguridad Seguridad de la información Roles y Responsabilidades 2. Tareas y condiciones del empleo Durante la ejecución del empleo 3. Gestión de activos 3.1 Clasificación de la información 3.2 Transferencia de medios de soportes físicos 3.7. Control de acceso a sistemas y aplicaciones 3. Restricción de acceso a la información 3. Requerimientos de conexión seguro 3.3 Mantenimiento de equipos	16	2	2	4	2	BAJO	BAJO	Mitigar el Riesgo	**1> Planificar la contratación de un Software Integral de Seguridad de la Información** **2> Realizar mantenimiento periódicos anos componentes de la entidad para garantizar el impacto y alcance del mismo** **3> Realizar mantenimiento periódico desde la supervisión que garantice mantener la gestión y avance del proyecto** **4> Realizar mesas de trabajo cuando que puedan evitar la ejecución del proyecto, para generar soluciones a corporatas inmediatas que garanticen la continuidad y culminación del proyecto**	Dirección Planeación Secretaria General Líderes de los Procesos de la entidad		