Unidad Solidaria

PLAN DE TRATAMIENTO DE RIESGOS

DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSI

2025

TABLA DE CONTENIDO

INTRODUCCIÓN

Uno de los principales activos en entidades Institucionales y empresas es la información y sus sistemas de información, razón por la cual tanto, se requiere un manejo adecuado en cuanto a la seguridad se refiere, y pueden encontrarse en diferentes medios o formas, y no solo en medios informáticos, se caracteriza por ser compleja e interdependiente. En la medida que se tenga una visión de los riesgos que la pueden afectar se pueden establecer controles y medidas efectivas, viables y transversales.

El punto de partida para la elaboración del Plan de Tratamiento de Riesgos del Sistema de Gestión de Seguridad y Privacidad de la información – **SGSI**– es identificar los activos de información de los procesos de la organización para determinar sus posibles vulnerabilidades y amenazas con el fin de evaluar los riesgos a los que están expuestos, y cómo pueden afectar sus actividades. Lo anterior permite generar los procedimientos adecuados para la administración de riesgos y a su vez generar un plan de tratamiento de riesgos.

La Unidad Administrativa Especial de Organizaciones Solidarias gestiona los riesgos de seguridad digital, de acuerdo como lo indica la política de administración del riesgo establecida por la entidad, se designa como responsable de la gestión de los riesgos de cada proceso al coordinador del grupo, en el caso de los riesgos de seguridad digital estos son identificados, y gestionados con la ayuda del Grupo de Tecnologías de la información, se busca cumplir con los lineamientos de la política de gobierno digital implementando lo definido en el habilitador de seguridad y privacidad de la información, se construye un plan de tratamiento de riesgos de seguridad y privacidad de la información que permite establecer controles en los riesgos de los activos de

información de los procesos identificados y evaluados, para preservar la confidencialidad, integridad, disponibilidad y privacidad de datos.

El Grupo de Tecnologías de la Información es el responsable de la elaboración, implementación del Plan de Tratamiento de Riesgos del Sistema de Gestión de Seguridad y Privacidad de la información – **SGSI**. Un factor para tener en cuenta son las personas encargadas de la custodia y manipulación de la información, por lo tanto, la socialización del plan a los funcionarios es importante para contar con su participación con el fin de proteger los activos de información de los procesos de la entidad.

Además, las acciones para implementar deben ser conocidas, tratadas y ejecutadas por la organización de una forma documentada, sistemática, estructurada y eficiente.

1. OBJETIVO

Implementar controles y alternativas de tratamiento de riesgos de seguridad y privacidad de la información para mitigar, aceptar, transferir o evitar el riesgo en los activos de información de los procesos con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de datos.

1.1 OBJETIVOS ESPECIFICOS

- Realizar seguimiento periódico a los controles.
- Evaluar las posibles acciones que se deben tomar para mitigar los riesgos de seguridad y privacidad de la información de acuerdo con los criterios definidos por la entidad.
- Involucrar a los líderes de los procesos de la entidad en la identificación, valoración, control y monitoreo de los riesgos de seguridad y privacidad de la información.

2. ALCANCE DEL DOCUMENTO

El Plan de Tratamiento de Riesgos del Sistema de Gestión de Seguridad y Privacidad de la información – **SGSI,** es aplicable a todos los procesos de la Unidad Solidaria, con alcance a los colaboradores de todos los niveles; Los líderes de los procesos deben contribuir con el seguimiento y control de los riesgos de los activos de información identificados, además de la implementación de las acciones definidas en el presente plan de tratamiento.

El tratamiento de riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales acciones, se cuenta con las siguientes opciones:

- Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

- Reducir el riesgo, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

- Compartir o transferir el riesgo, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la

información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

- Asumir un riesgo, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

3. GLOSARIO DE TÉRMINOS

Se relacionan algunos términos que se deben tener en cuenta en la elaboración, implementación y seguimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información.

- **Activo**

  Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56).

- **Activo cibernético**

  En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. (CONPES 3854).

- **Amenaza**

  Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).

- **Amenaza cibernética**

  Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).

- **Análisis de riesgo**

  Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

- **Ataque cibernético**

  Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

- **Ciberespacio**

  Ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Ciberseguridad**

  Conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y

tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

- **Control**

  Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- **Criterios del riesgo**

  Términos de referencia frente a los cuales se evalúa la importancia de un riesgo. (NTC ISO 31000:2011).

- **Delito cibernético**

  Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

- **Evaluación del control**

  Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).

- **Evaluación del riesgo**

  Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).

- **Evento de seguridad de la información**

  Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).

- **Fuente de riesgo**

  Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (NTC ISO 31000:2011).

- **Gestión del riesgo**

  Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011).

- **Gestión de riesgos de seguridad digital**

  Conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).

- **Identificación del riesgo**

  Proceso para encontrar, reconocer y describir el riesgo. (NTC ISO 31000:2011).

- **Incidente digital**

  Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

- **Incidente de seguridad de la información**

  Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

- **Inventario de activos**

  Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de Gestión de la Seguridad de la Información – SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).

- **Marco de referencia para la gestión del riesgo**

  Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo, a través de toda la organización. (NTC ISO 31000:2011).

- **Nivel de riesgo**

  Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad. (NTC ISO 31000:2011).

- **Plan para la gestión del riesgo**

  Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo. (NTC ISO 31000:2011).

- **Política para la gestión del riesgo**

  Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

- **Proceso para la gestión del riesgo**

  Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo. (NTC ISO 31000:2011).

- **Reducción del riesgo**

  Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).

- **Retención del riesgo**

  Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

- **Riesgo**

  Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).

- **Riesgo inherente**

  Situación a la que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).

- **Riesgo residual**

  Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011).

- **Seguridad de la información**

  Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).

- **Seguridad digital**

  Situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).

- **Sistema para la gestión del riesgo**

  Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo. (NTC ISO 31000:2011).

- **Valoración del riesgo**

  Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

- **Vulnerabilidad**

  Debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

4. CONTEXTO

En virtud de la implementación de la política de administración de riesgos de la entidad, se realiza en el año 2022 un trabajo de grupo con los líderes de los procesos para identificar los riesgos de seguridad y privacidad de la información en los procesos de la Unidad Solidaria, se hace la valoración de los controles de los procesos generando la calificación de solidez del conjunto de controles, encontrando que aún les falta mejorar en la efectividad por parte de los líderes de proceso por lo que se requiere fortalecer mediante las auditorías y demás recursos de gestión la efectividad de estos.

El Grupo de Planeación y Estadística de la Unidad se basa en la guía de administración de riesgos de la función pública para orientar la elaboración de la matriz de riesgos de seguridad digital de la entidad.

ID	Riesgo	Activo	Tipo	Amenaza	Vulnerabilidades
1	Pérdida de la Disponibilidad y Confidencialidad	DNS Servidores de red Firewall Red TCP/IP	Seguridad Digital	Acceso a la red o a los sistemas de información por personas no autorizadas	Desactualización o daño del Firewall
					Conexiones remotas no seguras
					Contraseñas predeterminadas no modificadas
					Mantenimiento inadecuado
					Falta de formación y conciencia sobre seguridad de la información
2	Pérdida de la Disponibilidad y Confidencialidad e Integridad	Sistemas de información File Server Servidores Físicos Servidores Virtuales	Seguridad Digital	Pirata informático intruso ilegal Errores de mantenimiento Mal funcionamiento de equipos	Conexión a escritorio remoto no segura
					Carencia de parches de seguridad de los sistemas operativos
					Dispositivos IoT inseguros
					Equipos de escritorio y servidores sin antivirus
					Equipos con sistemas operativos obsoletos
					Usuarios incapacitados en temas de seguridad de la información
3	Pérdida de la Disponibilidad y Confidencialidad e Integridad	Bases de datos nómina Matriz personas beneficiadas Matriz organizaciones solidarias	Seguridad Digital	Código Malicioso Fuga de información	Conexión a escritorio remoto no segura
					Carencia de parches de seguridad de los sistemas operativos
					Dispositivos IoT inseguros

					Equipos de escritorio y servidores sin antivirus
					Equipos con sistemas operativos obsoletos
					Usuarios incapacitados en temas de seguridad de la información
4	Pérdida de la Disponibilidad y Confidencialidad e Integridad	Sistema de gestión documental SGDEA	Seguridad Digital	Malversación y fraude Destrucción de registros Falsificación de registros	Contraseñas predeterminadas no modificadas
					Control inadecuado del acceso físico
					Inadecuada gestión y protección de contraseñas
					Protección física no apropiada
5	Pérdida de la Disponibilidad y Confidencialidad e Integridad	Expedientes de Jurídica, gestión documental Historias Laborales	Seguridad Digital	Destrucción de registros Desastre natural, incendio, inundación, rayo. Revelación de Información Cambios no autorizados de registros	Ubicación vulnerable a inundaciones
					Control inadecuado del acceso físico
					Respaldo inapropiado o irregular
					Protección física no apropiada

5. PLAN DE ACCIÓN

De acuerdo con la matriz de riesgos de seguridad digital aprobada donde se definieron los controles para la mitigación de los riesgos, se elaboró el Plan de Tratamiento de Riesgos del Sistema de Gestión de Seguridad y Privacidad de la información – **SGSI** de la Unidad Solidaria para el año 2025.

Riesgo	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento
Pérdida de la Disponibilidad y Confidencialidad	Realizar seguimiento y monitorio mensual al Firewall	Profesional Especializado	1-abril-25	Mensual
	* Realizar verificación de software no autorizado dentro de las actividades programadas en el plan de mantenimiento	Grupo TI	1-abril-25	Mensual
	* Realizar verificación de software no autorizado dentro de las actividades y solicitudes de mantenimiento realizadas por los ingenieros del grupo TI.			
	* Seguimiento al Plan de Seguridad y Privacidad de la Información	Coordinador Grupo de Tecnologías de la Información y Profesional Especializado	1-abril-25	Cuatrimestral
	* Administración del Control de Acceso por el aplicativo Biométrico			
	* Realizar verificación de actualización de permisos de acceso a los roles de administrador	Coordinador Grupo de Tecnologías de la Información y Profesional Especializado	1-abril-25	Semestral
	* Ejecución del Plan de Mantenimiento de la infraestructura tecnológica	Profesional Especializado	1-abril-25	Mensual
	* Realizar seguimiento a los procesos de contratación de mantenimiento			

	* Ejecución del Plan de sensibilización y comunicaciones	Grupo TI	1-abril-25	Mensual
Pérdida de la Disponibilidad y Confidencialidad e Integridad	* Realizar verificación de software no autorizado dentro de las actividades programadas en el plan de mantenimiento	Grupo TI	1-abril-25	Mensual
	* Realizar verificación de software no autorizado dentro de las actividades y solicitudes de mantenimiento realizadas por los ingenieros del grupo TI.			
	* Realizar las actualizaciones de software (Parches de seguridad, firmware, Sistemas operativos, Servicios, Módulos) de la infraestructura tecnológica. Reporte de actualizaciones de software	Grupo TI	1-abril-25	Cuatrimestral
	* Revisión de la instalación del software antivirus desde la consola de administrador del antivirus	Grupo TI	1-abril-25	Mensual
	* Verificación de software antivirus dentro de las actividades y solicitudes de mantenimiento realizadas por los ingenieros del grupo TI.			
	* Reporte de vida útil y de deterioro de los activos tangibles de la entidad	Coordinador Grupo de Tecnologías de la Información	1-abril-25	Semestral
	* Revisión de reportes de ataques de malware desde la consola de administrador del antivirus	Profesional Especializado y Profesional Universitario Grado 7	1-abril-25	Mensual
	* Revisión de reportes de ataques informáticos desde el monitorio del Firewall			
	* Envió de Tips de Seguridad y ejecución del plan de sensibilización y comunicaciones	Grupo TI	1-abril-25	Mensual
Pérdida de la Disponibilidad y Confidencialidad e Integridad	* Realizar verificación de software no autorizado dentro de las actividades programadas en el plan de mantenimiento	Grupo TI	1-abril-25	Mensual

	* Realizar verificación de software no autorizado dentro de las actividades y solicitudes de mantenimiento realizadas por los ingenieros del grupo TI.	Grupo TI	1-abril-25	Mensual
	* Realizar las actualizaciones de software (Parches de seguridad, firmware, Sistemas operativos, Servicios, Módulos) de la infraestructura tecnológica. Reporte de actualizaciones de software	Grupo TI	1-abril-25	Cuatrimestral
	* Revisión de la instalación del software antivirus desde la consola de administrador del antivirus	Grupo TI	1-abril-25	Mensual
	* Verificación de software antivirus dentro de las actividades y solicitudes de mantenimiento realizadas por los ingenieros del grupo TI.			
	* Revisión de reportes de ataques de malware desde la consola de administrador del antivirus	Profesional Especializado y Profesional Universitario Grado 7	1-abril-25	Mensual
	* Revisión de reportes de ataques informáticos desde el monitorio del Firewall			
	* Revisión de reportes de ataques de malware desde la consola de administrador del antivirus	Profesional Especializado y Profesional Universitario Grado 7	1-abril-25	Mensual
	* Revisión de reportes de ataques informáticos desde el monitorio del Firewall			
	* Envió de Tips de Seguridad y ejecución del plan de sensibilización y comunicaciones	Grupo TI	1-abril-25	Mensual
Pérdida de la Disponibilidad y Confidencialidad e Integridad	* Realizar verificación de actualización de permisos de acceso a los roles de administrador.	Coordinador Grupo de Tecnologías de la Información y Profesional Especializado	1-abril-25	Semestral

	* Administración del Control de Acceso por el aplicativo Biométrico	Coordinador Grupo de Tecnologías de la Información	1-abril-25	Cuatrimestral
Pérdida de la Disponibilidad y Confidencialidad e Integridad	* Seguimiento al Plan de Seguridad y Privacidad de la Información	Profesional Especializado	1-abril-25	Cuatrimestral
	* Seguimiento al Plan de Seguridad y Privacidad de la Información	Coordinador Grupo de Tecnologías de la Información y el Profesional Especializado	1-abril-25	Cuatrimestral
	* Administración del Control de Acceso por el aplicativo Biométrico			
	* Realización y verificación de las estrategias de copias de seguridad de información	Profesional Universitario Grado 7	1-abril-25	Mensual
	* Revisión de cámaras de Seguridad	Coordinador Grupo de Tecnologías de la Información	1-abril-25	Cuatrimestral
	* Administración del Control de Acceso por el aplicativo Biométrico			

El grupo de tecnologías de la información se encarga de la implementación y seguimiento del desarrollo del plan de acción y reporta los resultados a la coordinación del grupo de planeación y estadística.

Una vez al año se debe hacer reunión con los líderes de los procesos para revisar y establecer los ajustes necesarios de los riesgos de seguridad y privacidad de la información en los procesos de la Unidad Solidaria y la valoración de los controles de los procesos para actualizar la calificación de solidez del conjunto de controles.

JOSE IGNACIO HERRERA TRUJILLO
Coordinador – Grupo de Tecnologías de la Información

Verificó: Wilson Antonio Daza Pavajeau – contratista Gobierno en Línea.

Aprobó: Nombre Director Técnico.