PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN
Vigencia de 2022

Departamento Administrativo para la Prosperidad Social.
Bogotá D.C. – Colombia.
enero de 2022

CONTENIDO

1. INTRODUCCIÓN

Teniendo en cuenta La Política de Gobierno Digital como un componente del Modelo Integrado de Planeación y Gestión MIPG, la entidad acogiendo los lineamientos y mejores prácticas establecidas en diferente Normatividad, para la Vigencia 2022 realizarán las actividades descritas en el presente plan, el cual forma parte integral del Plan de Acción Institucional de Prosperidad Social.

2. OBJETIVO

Definir el plan de Tratamiento de Riesgos de seguridad de la información para el año 2022 con el fin de garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de los activos de información en Prosperidad Social.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Seguridad de la Información de Prosperidad Social para la vigencia 2022, está orientado a gestionar los riesgos de seguridad digital asociados a los activos de información, sistemas de información, plataforma tecnológica y servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de los diferentes procesos de operación en la Entidad.

4. Definiciones

Amenazas: Situación potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización.

Confidencialidad: Propiedad de la información que la hace no disponible ósea divulgada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de exactitud y completitud.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad o personas autorizadas.

Riesgo de Seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo Inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo Residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

5. REFERENCIAS NORMATIVAS

- ✓ Ley 87 de 1993. establece normas para el ejercicio del control interno en las entidades y organismos del Estado.
- ✓ Ley 489 de 1998. dicta normas sobre la organización y funcionamiento de las entidades del orden nacional.
- ✓ Ley 1474 de 2011. dicta normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- ✓ Decreto 1537 de 2001 - Artículo 4 Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado.
- ✓ Decreto 1083 de 2015. Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
- ✓ Decreto 1499 de 2017 modifica el Decreto Único reglamentario del sector función pública.
- ✓ CONPES 3995 DE 2020: Política Nacional de Confianza y Seguridad Digital
- ✓ NORMA ISO 27001:2013 Es un estándar para los Sistemas Gestión de la Seguridad de la Información que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.
- ✓ Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- ✓ Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

6. VISIÓN GENERAL DEL PROCESO DE GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

La metodología a través de la cual se gestionan los riesgos es la definida por la Entidad a través de la “Guía para Administración de Riesgos”, la cual a su vez tiene alineación con la Guía para la administración del riesgo del Departamento Administrativo de la Función Pública

Fuente propia

7. SITUACIÓN ACTUAL

Para el año 2022 se inicia con veinte (20) Riesgos de seguridad de la información, tipificados como riesgos de seguridad digital e integrados en la Mapa Institucional de riesgos de prosperidad Social. Estos riesgos vienen siendo gestionados con la implementación de controles del Anexo A de la norma ISO 27001 para disminuir el nivel de riesgo a niveles aceptables.

8. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta el Mapa de Riesgos Institucional, específicamente en los riesgos relacionados con la seguridad de la Información, los cuales están categorizados como seguridad Digital, se seleccionan los controles para mitigar los riesgos inherentes identificados en la Entidad relacionados con la seguridad Digital. Dichos controles forman parte de los Dominios establecidos en el Anexo A de la Norma ISO 27001:2013.

De otra parte y con el fin de dar cumplimiento a los objetivos del SGSI, es necesario realizar las siguientes actividades teniendo en cuenta que algunas de ellas están en etapa de implementación, actualización de controles y/o se deben implementar:

	Controles Seleccionados	Descripción de actividades
• A.6.1.3	• Contacto con las autoridades	Establecer grupos de interés y definir puntos de contacto
• A.8.1.1	• Inventario de activos tecnológicos y de la información.	Revisar el cumplimiento de la metodología para la gestión de activos. Implementar los mecanismos disponibles para mantenimiento y actualización del inventario de activos de información.
• A.8.1.3	• Uso aceptable de los activos tecnológicos	Diseñar y llevar a cabo campañas periódicas para sensibilizar a los usuarios sobre la aplicación de la política de uso aceptable de recursos tecnológicos de la entidad.
• A.8.2.1	• Clasificación de la información	Evaluar el nivel de aplicación de la guía de clasificación de información que contempla niveles de sensibilidad distintos e indica el tratamiento que debe tener la información de acuerdo con su criticidad.
• A.7.2.3	• Procesos disciplinarios	Continuar con la Implementación de la política y/o procedimiento para los procesos disciplinarios asociados a incidentes de seguridad.
• A.8.1.4	• Devolución de activos tecnológicos • Eliminación, destrucción y reutilización de equipos	Validar el nivel de implementación de la política de borrado seguro y de devolución de activos.

• A.11.1.1 • A.11.1.2 • A.11.1.3 • A.11.1.4 • A.11.1.5 • A.11.1.6	• Controles físicos de entrada • Aseguramiento de oficinas, cuartos e instalaciones • Trabajo en áreas restringidas / seguras • Acceso público, envíos y áreas de carga	Evaluar la eficiencia de las puertas de control de acceso y el procedimiento de ingreso de invitados/visitantes. Evaluar el nivel de cultura organizacional, para fomentar el uso del carné de los colaboradores de la entidad. Revisar la seguridad física de los servidores y las estaciones críticas de trabajo. Validar la cobertura de la instalación de cámaras de seguridad en el área de procesamiento de datos.
	• Aseguramiento de oficinas, cuartos e instalaciones	Revisar la seguridad física de los servidores y las estaciones de trabajo.
	• Protección contra amenazas externas y ambientales	Revisar el funcionamiento y gestión del sistema de aire acondicionado y sistemas de detección y extinción de incendios.
	• Ubicación y protección de equipos tecnológicos	Revisar la seguridad física de los servidores y las estaciones de trabajo.
• A.11.2.4	• Mantenimiento de los equipos	Continuar el programa de mantenimiento para los componentes físicos de infraestructura donde se establece periodicidad del mantenimiento correctivo en función del tipo de activo.
• A.12.4.1 • A.12.4.2 • A.12.4.3 • A.12.4.4	• Registros de Auditoría • Monitoreo del uso del sistema • Protección de registros de monitoreo • Registros de monitoreo de administradores y operadores	Verificar la implementación de la política de auditoría, frecuencia de revisión, el alcance de cada auditoría a los sistemas de información y el período de retención de los registros establecidos.
		Comprobar el cumplimiento de la política de monitoreo al uso de sistemas, garantizando el seguimiento a actividades propias de la entidad.
		Evidenciar el cumplimiento a la política de monitoreo, verificar las condiciones de almacenamiento y custodia que se establecen para los registros de monitoreo.

		Implementar la política que estipule las condiciones sobre las cuales se deba hacer el monitoreo al uso de sistemas por parte de administradores y operadores garantizando el seguimiento a actividades propias de la Entidad.
• **A.8.3.3**	• Medios físicos en tránsito	Validar el cumplimiento de la política para el transporte de información en medios físicos.
• **A.12.3.1**	• Respaldo de la información.	Evaluar el cumplimiento de la política de Back up para la información. Revisar la actualización de las tablas de retención documental de acuerdo a los activos de información establecidos para el alcance.
• **A.14.1.3**	• Seguridad de la documentación de los sistemas intercambio de información.	Validar que los sistemas de información cuenten con los manuales de usuario y técnicos y que la documentación asociada a los mismos sea accesible por las personas que la requieren .
• **A.14.2**	• Sistemas de información de la entidad	Confirmar el cumplimiento a la política para la conexión segura a sistemas de información de la entidad: Perfiles de acceso, clasificación de información, acceso a información sensible, identificación y mitigación de vulnerabilidades conocidas. Validar la ejecución segura de programas autorizados por medio de HIPS, APP control y Firewall para servidores, según el caso.
• **A.14.2.9**	• Aceptación de sistemas	Verificar el cumplimiento a la política de aceptación de sistemas de información, que incluye entre otros: documentaciones asociadas, pruebas de seguridad, fiabilidad de la arquitectura, entre otros.
• **A.8.3.1**	• Gestión de medios removibles	Evaluar el cumplimiento de la política de gestión de medios removibles que determine las condiciones y la forma como se permitirá la utilización de dispositivos extraíbles. Adopción de cifrado en medios removibles .
• **A.11.2.7**	• Destrucción de medios	Confirmar el cumplimiento a la política de borrado seguro que defina el procedimiento, herramientas y mecanismos de verificación aplicables para casos de destrucción de medios.

• A.6.2.2	• Teletrabajo / trabajo remoto	Verificar la aplicación de la política para el trabajo remoto o trabajo en casa, como está establecido en la Entidad.
• A.9.1.1 • A.9.1.2	• Política de Control de Acceso	Revisar que en las aplicaciones y en los sistemas de información se encuentre implementada la política de control de acceso lógico, que determine los requisitos para la autorización de permisos, la segregación de perfiles en cada caso, separación de funciones (SoD), periodos de revisión de permisos, entre otros.
• A.9.2.1 • A.9.2.2 • A.9.2.3 • A.9.2.4 • A.9.2.5	• Registro de Usuarios y Gestión de privilegios	Validar el cumplimiento del procedimiento para la asignación y revocación de privilegios de usuario, al igual que los registros para cada operación de administración. Revisar que, cada vez que se retira o desvincula de la entidad una persona, se le debe desactivar las cuentas que tenía asignadas. En el sistema de control biométrico es posible que existan usuarios habilitados, de personas que ya no trabajan en la entidad. Se debe hacer un chequeo en profundidad del tema, para depurar UsersIDs que ya no se requieren en éste y en los demás sistemas. Verificar que se realice comparación exhaustiva en cada uno de los componentes de sistemas (Aplicaciones y Dominio), para depurar y borrar aquellos usuarios que ya no laboran en la entidad. Verificar que, en los aplicativos y sistemas de información, se bloquee después de intentos fallidos de acceso y permanezca bloqueada por un tiempo determinado o hasta que un rol administrador la desbloquee.

• A.9.4.3	• Gestión y uso de Contraseñas (passwords)	Validar que en las aplicaciones y sistemas de información se estipulen los requisitos mínimos para la creación, transmisión y cambio de contraseñas. sensibilizar a usuarios y administradores sobre la aplicación de esta política.
• A.9.1.2	• Políticas para el uso de los servicios de la red de datos	Verificar el cumplimiento de la política de uso aceptable de activos, los aspectos relacionados a uso de la red, equipos entre otros.
• A.13.1.1	• Identificación de equipos en la red	Definir mecanismos para la identificación de equipos corporativos y externos en la red. Aplicar a cada uno un tratamiento diferente de acuerdo a las necesidades.
• A.13.1.3	• Separación en la red	Revisar y evaluar el nivel de la segregación de redes actual.
• A.9.1.2	• Control de conexión a la red de trabajo	Verificar la implementación de la política de acceso y conexión la red LAN y WAN de la Entidad
• A.13.1.1	• Control de enrutamiento de red	Validar las políticas de enrutamiento actuales a la luz de las buenas prácticas de seguridad.
• A.14.2.4	• Restricciones a cambios en paquetes de software	Implementar la política y procedimiento de gestión de cambios
• A.12.6.1	• Control técnico de vulnerabilidades	Revisar semestralmente las vulnerabilidades técnicas conocidas, valorarlas de acuerdo a la metodología de riesgos y tratarlas con prioridad de acuerdo a criticidad del activo. Hacer escaneo de vulnerabilidades que incluyan diferentes pruebas de intrusión.
• A.12.5	• Control del software operacional(operativo)	Implementar la política y procedimiento de gestión de cambios.
• A.14.2.2	• Procedimientos para el control de cambios	Implementar la política y procedimiento de gestión de cambios.
• A.14.2.3	• Revisión técnica de aplicaciones después de cambios al sistema operativo	Implementar la política y procedimiento de gestión de cambios que incluya revisión de cambios aplicados, plan de roll back, plan de contingencia, entre otros.

• **A.14.2.1**	• Validación de los datos de entrada	Efectuar la validación de parámetros de entrada a aplicativos desde una perspectiva ofensiva utilizando buenas prácticas para revisión de software (OWASP)
	• Control del procesamiento interno	Definir mecanismos de validación de integridad utilizando HASH, Checksum o algún mecanismo fiable.
	• Integridad de los mensajes	Definir mecanismos de validación de integridad utilizando HASH, Checksum o algún mecanismo fiable.
	• Validación de los datos de salida	Definir directrices para la prueba de salidas de sistemas de acuerdo a OWASP.
• **A.10.1.1**	• Política para el uso de controles criptográficos	Validar la aplicación de la política de cifrado que dé cumplimiento a la legislación aplicable, mediante la utilización de protocolos como SSL/TLS, IPSEC, SSH, entre otros.
• **A.10.1.2**	• Gestión de llaves	Implementar la política para la gestión de llaves: generación, distribución, revocación y demás.
• **A.18.2.3**	• Verificación del cumplimiento técnico	Revisar el cumplimiento del manual de políticas de seguridad de la información.