



La equidad  
es de todos

Prosperidad  
Social

# PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

Departamento Administrativo para la Prosperidad Social.  
Bogotá D.C. – Colombia.  
enero de 2021

## 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 2021 realizarán las actividades descritas en el presente plan, el cual forma parte integral del Plan de Acción Institucional de Prosperidad Social.

## OBJETIVO

Definir el plan de Tratamiento de Riesgos de seguridad de la información para el año 2021 con el fin de preservar los criterios de confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información en Prosperidad Social.

## 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
<ul style="list-style-type: none"> <li>Auditoría interna</li> </ul>	Programar una auditoría interna al SGSI alineada a la norma ISO27001:2013, con el fin de continuar con el proceso de certificación en dicha Norma para otros procesos Misionales-Estratégicos de la Entidad incluidos en Equidad Digital.
<ul style="list-style-type: none"> <li>Contacto con las autoridades</li> </ul>	Establecer grupos de interés y definir puntos de contacto
<ul style="list-style-type: none"> <li>Inventario de activos tecnológicos y de la información.</li> <li>Responsables de los activos tecnológicos</li> </ul>	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.

<ul style="list-style-type: none"> <li>• Uso aceptable de los activos tecnológicos</li> </ul>	<p>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.</p>
<ul style="list-style-type: none"> <li>• Normas para clasificación de la información</li> <li>• Identificación y Manejo de la información</li> </ul>	<p>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.</p>
<ul style="list-style-type: none"> <li>• Procesos disciplinarios</li> </ul>	<p>Continuar con la Implementación de la política y/o procedimiento para los procesos disciplinarios asociados a incidentes de seguridad.</p>
<ul style="list-style-type: none"> <li>• Devolución de activos tecnológicos</li> <li>• Eliminación, destrucción y reutilización de equipos</li> </ul>	<p>Validar el nivel de implementación de la política de borrado seguro y de devolución de activos.</p>
<ul style="list-style-type: none"> <li>• Controles físicos de entrada</li> <li>• Aseguramiento de oficinas, cuartos e instalaciones</li> <li>• Trabajo en áreas restringidas / seguras</li> <li>• Acceso público, envíos y áreas de carga</li> </ul>	<p>Evaluar la eficiencia de las puertas de control de acceso y el procedimiento de ingreso de invitados/visitantes.</p> <p>Evaluar el nivel de cultura organizacional, para fomentar el uso del carné de los colaboradores de la entidad.</p> <p>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.</p>
<ul style="list-style-type: none"> <li>• Aseguramiento de oficinas, cuartos e instalaciones</li> </ul>	<p>Revisar la seguridad física de los servidores y las estaciones de trabajo.</p>
<ul style="list-style-type: none"> <li>• Protección contra amenazas externas y ambientales</li> </ul>	<p>Revisar el funcionamiento y gestión del sistema de aire acondicionado y sistemas de detección y extinción de incendios.</p>
<ul style="list-style-type: none"> <li>• Ubicación y protección de equipos tecnológicos</li> </ul>	<p>Revisar la seguridad física de los servidores y las estaciones de trabajo.</p>
<ul style="list-style-type: none"> <li>• Mantenimiento de los equipos</li> </ul>	<p>Continuar el programa de mantenimiento para los componentes físicos de infraestructura donde se establece periodicidad del mantenimiento correctivo en función del tipo de activo.</p>



## PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

<ul style="list-style-type: none"><li>• Registros de Auditoría</li><li>• Monitoreo del uso del sistema</li><li>• Protección de registros de monitoreo</li><li>• Registros de monitoreo de administradores y operadores</li></ul>	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.
<ul style="list-style-type: none"><li>• Medios físicos en tránsito</li></ul>	Validar el cumplimiento de la política para el transporte de información en medios físicos.
<ul style="list-style-type: none"><li>• Registro de fallas</li></ul>	Revisar la efectividad del sistema de registro y almacenamiento de fallas para los activos de información. Verificar la creación de la base de datos de conocimiento (KDB)
<ul style="list-style-type: none"><li>• Respaldo de la información.</li></ul>	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.
<ul style="list-style-type: none"><li>• Seguridad de la documentación de los sistemas intercambio de información.</li></ul>	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 .
<ul style="list-style-type: none"><li>• Sistemas de información de la entidad</li></ul>	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.



<ul style="list-style-type: none"><li>• Aceptación de sistemas</li></ul>	Verificar el cumplimiento a la política de aceptación de sistemas de información, que incluye entre otros: documentación asociadas, pruebas de seguridad, fiabilidad de la arquitectura, entre otros.
<ul style="list-style-type: none"><li>• Gestión de medios removibles</li></ul>	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 .
<ul style="list-style-type: none"><li>• Destrucción de medios</li></ul>	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.
<ul style="list-style-type: none"><li>• Teletrabajo / trabajo remoto</li></ul>	Verificar la aplicación de la política para el trabajo remoto o trabajo en casa, como está establecido en la Entidad.
<ul style="list-style-type: none"><li>• Política de Control de Acceso</li></ul>	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.
<ul style="list-style-type: none"><li>• Registro de Usuarios y Gestión de privilegios</li></ul>	<p>Validar el cumplimiento del procedimiento para la asignación y revocación de privilegios de usuario, al igual que los registros para cada operación de administración.</p> <p>Revisar que, cada vez que se retira o desvincula de la entidad una persona, se le debe desactivar las cuentas que tenía asignadas.</p> <p>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.</p> <p>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.</p> <p>Verificar que, en los aplicativos y sistemas de información, se bloquee después de intentos fallidos de acceso y permanezca bloqueada por un tiempo</p>

	determinado o hasta que un rol administrador la desbloquee.
<ul style="list-style-type: none"> <li>Gestión y uso de Contraseñas (passwords)</li> </ul>	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.
<ul style="list-style-type: none"> <li>Autenticación de usuarios para conexiones externas</li> </ul>	Revisar el cumplimiento de la política para el uso de conexiones seguras alternas: VPN. Evaluar la posibilidad de tener múltiples factores de autenticación.
<ul style="list-style-type: none"> <li>Identificación y autenticación de los usuarios.</li> </ul>	Fortalecer el proceso de autenticación de usuarios con factores de autenticación robustos.
<ul style="list-style-type: none"> <li>Políticas para el uso de los servicios de la red de datos</li> </ul>	Verificar el cumplimiento de la política de uso aceptable de activos, los aspectos relacionados a uso de la red, equipos entre otros.
<ul style="list-style-type: none"> <li>Identificación de equipos en la red</li> </ul>	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.
<ul style="list-style-type: none"> <li>Diagnóstico remoto y protección de la configuración de puertos</li> </ul>	Validar la apertura de los puertos que son estrictamente necesarios para el funcionamiento de los sistemas de información.
<ul style="list-style-type: none"> <li>Separación en la red</li> </ul>	Revisar y evaluar el nivel de la segregación de redes actual.
<ul style="list-style-type: none"> <li>Control de conexión a la red de trabajo</li> </ul>	Verificar la implementación de la política de acceso y conexión la red LAN y WAN de la Entidad
<ul style="list-style-type: none"> <li>Control de enrutamiento de red</li> </ul>	Validar las políticas de enrutamiento actuales a la luz de las buenas prácticas de seguridad.
<ul style="list-style-type: none"> <li>Restricciones a cambios en paquetes de software</li> </ul>	Implementar la política y procedimiento de gestión de cambios
<ul style="list-style-type: none"> <li>Control técnico de vulnerabilidades</li> </ul>	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.

<ul style="list-style-type: none"> <li>Control del software operacional(operativo)</li> </ul>	Implementar la política y procedimiento de gestión de cambios.
<ul style="list-style-type: none"> <li>Procedimientos para el control de cambios</li> </ul>	Implementar la política y procedimiento de gestión de cambios.
<ul style="list-style-type: none"> <li>Revisión técnica de aplicaciones después de cambios al sistema operativo</li> </ul>	Implementar la política y procedimiento de gestión de cambios que incluya revisión de cambios aplicados, plan de roll back, plan de contingencia, entre otros.
<ul style="list-style-type: none"> <li>Validación de los datos de entrada</li> </ul>	Efectuar la validación de parámetros de entrada a aplicativos desde una perspectiva ofensiva utilizando buenas prácticas para revisión de software (OWASP)
<ul style="list-style-type: none"> <li>Control del procesamiento interno</li> </ul>	Definir mecanismos de validación de integridad utilizando HASH, Checksum o algún mecanismo fiable.
<ul style="list-style-type: none"> <li>Integridad de los mensajes</li> </ul>	Definir mecanismos de validación de integridad utilizando HASH, Checksum o algún mecanismo fiable.
<ul style="list-style-type: none"> <li>Validación de los datos de salida</li> </ul>	Definir directrices para la prueba de salidas de sistemas de acuerdo a OWASP.
<ul style="list-style-type: none"> <li>Política para el uso de controles criptográficos</li> </ul>	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.
<ul style="list-style-type: none"> <li>Gestión de llaves</li> </ul>	Implementar la política para la gestión de llaves: generación, distribución, revocación y demás.
<ul style="list-style-type: none"> <li>Verificación del cumplimiento técnico</li> </ul>	Revisar el cumplimiento del manual de políticas de seguridad de la información.