SUBSECRETARIA GENERAL

PLAN DE GESTION DE RIESGOS - SEGURIDAD DE LA INFORMACIÓN

Vigencia 2022

INTRODUCCIÓN

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de estos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de la Secretaria Distrital de Hacienda.

Se deben tener en cuenta algunas de las siguientes consideraciones, independientemente, interrelacionadas o en conjunto:

- **Evitar:** es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.
- **Prevenir:** corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.
- **Reducir o mitigar:** corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo.
- **Dispersar:** es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos.
- **Compartir:** es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

El documento CONPES 3995 del 01 de julio de 2020, estableció la Política Nacional de Confianza y Seguridad Digital que tiene por objetivo: *"Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías."*.[1]

1 Tomado del CONPES 3995 del 01 de julio de 2020 - numeral 5.1 objetivo general de Seguridad y Privacidad de la Información – numeral 8.2.1

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, siguiendo los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020, del Departamento Administrativo de la Función Pública, se debe realizar el análisis de los controles con el dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados", la Secretaria Distrital de Hacienda reconociendo la información como un activo, se alinea a las definiciones y lineamientos de la gestión de riesgos, mediante la aplicación de procedimientos y controles requeridos para la protección de la información, en particular los establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

La Subsecretaría General y la Oficina de Análisis y Control de Riesgo, realizarán el seguimiento a la implementación de este plan que se presenta este documento para conocimiento de la ciudadanía, órganos de control y demás partes interesadas.

Objetivo y alcance del documento.

El presente documento describe en forma macro el plan actividades enfocado en la gestión de riesgos de seguridad de la información en la Secretaria Distrital de Hacienda, el plan está basado en la matriz elaborada por la Oficina de Análisis y Control de Riesgo de la SDH y revisada en conjunto con Seguridad de la Información, la Dirección de Informática y Tecnología; el desarrollo del plan incluirá la implementación de los controles de los planes de tratamiento de riesgos, para posteriormente efectuar el seguimiento y plan de mejora si aplica.

Marco en el que se desarrolla este plan. La entidad en este momento se encuentra en la etapa inicial de una nueva administración, la cual en su plan de gobierno contempla 5 metas, de las cuales dos de ellas están relacionadas con riesgos sobre la información, estas son;

- ¡Vivir sin miedo!
- ¡Con oportunidades, empleo y educación somos imparables!

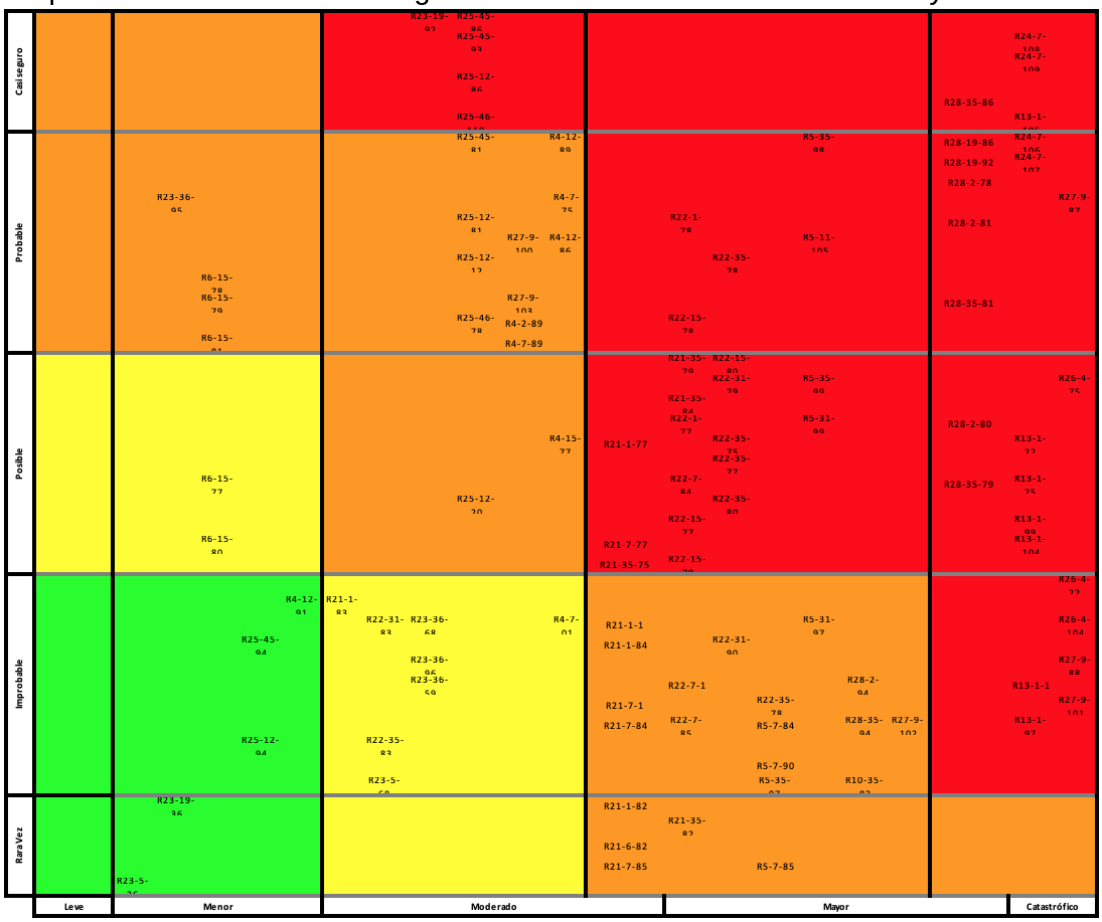
Vivir sin miedo. Desde la perspectiva de la subsecretaría general la seguridad es un aspecto que también debe ser inherente a los servicios digitales, razón por la cual la gestión de riesgos tecnológicos son la base de plan, así como la protección de la información de la ciudadanía.

Con oportunidades, empleo y educación somos imparables. Esta meta contempla el cuidado de lo público, incentivando el uso de la tecnología y nuevas herramientas digitales, en este sentido el plan de seguridad contempla la inclusión de controles automáticos en la plataforma SAP, conforme a los riesgos identificados y que requieren la definición de un plan de mitigación.

Como antecedentes, tenemos que la entidad ha dado importantes avances en la gestión riesgos, identificando las vulnerabilidades y asociándolas a amenazas, de manera que los riesgos sean evaluados, calificados y priorizados para determinar la importancia de su tratamiento. El ciclo anteriormente descrito obedece a las mejores prácticas en la materia y en particular en aplicación a la Guía 7, anteriormente mencionada.

A continuación se presenta una vista gerencial de la matriz de riesgo de seguridad de la información de la SDH y de algunos de los elementos o aspectos que fueron aplicados en su elaboración:

1. Mapa de calor. La siguiente es la distribución del riesgo residual, como se aprecia prácticamente todos los riesgos están ubicados en el nivel extremo y alto.



Amenazas más representativas. Las siguientes son las amenazas más representativas que aparecen en la matriz de riesgo.

- Abuso de derechos de usuario.

- Acceso a red y/o sistemas de información por usuario no autorizado.
- Perdida de suministro de energía.
- Mal uso de recursos.
- Exposición de datos y/o documentos.

En cuanto a los criterios parar calificar la probabilidad, se tomaron los niveles establecidos por el DAFP, en su guía para la administración del riesgo y el diseño de controles en entidades públicas (versión 4 octubre de 2018), la cual se muestra a continuación:

CRITERIOS DE VALORACIÓN PROBABILIDAD		
Nivel	**HIPOTÉTICA**	**EXPOSICIÓN**
Casi seguro	Ocurre en la mayoría de las circunstancias o se tiene la suficiente información para determinar una frecuencia muy alta.	Constantemente se presentan situaciones de exposición, que normalmente conllevan a la materialización del riesgo.
Probable	Probablemente ocurre la mayoría de las veces o se tiene la suficiente información para determinar una frecuencia alta.	A menudo se presentan situaciones de exposición, que pueden conllevar a la materialización del riesgo varias veces en la entidad.
Posible	Alguna posibilidad de que el evento ocurra o no se tiene la información suficiente para determinar su ocurrencia.	Algunas veces se presentan situaciones de exposición, de las cuales es posible que conlleven a la materialización del riesgo alguna vez.
Improbable	Puede ocurrir en circunstancias ocasionales o existe la suficiente información para determinar una frecuencia baja.	Ocasionalmente se presentan situaciones de exposición, de las cuales no se espera que conlleve a la materialización del riesgo, aunque puede ser concebible.
Rara vez	Puede ocurrir en circunstancias excepcionales o existe toda la información para determinar una frecuencia muy baja.	Eventualmente se presentan situaciones de exposición que pueden conllevar a la materialización del riesgo.

2. Controles sugeridos en los planes de mitigación para tener un nivel aceptable de riesgo.

Conforme a lo establecido en Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020, la mitigación de riesgo requerirá la adopción de controles y en forma preliminar la Oficina de Análisis y Control de Riesgo identifica controles susceptibles de implementar los cuales serán tenidos en cuenta en las

mesas de trabajo a adelantar con los líderes de proceso. En el Anexo A se relacionan los controles asociados a los riesgos identificados.

3. Actividades para realizar en la vigencia 2022.

Este plan permite mitigar y controlar vulnerabilidades identificadas para tal fin se establece el siguiente cronograma:

CV	Lista de Vulnerabilidades	Opción de Control	Descripción del Tratamiento	Responsable	Fecha de Implementación	Responsable de Aprobación
V01	Préstamo de usuarios y claves de acceso a sistemas de información, servicios en línea, sistemas operativos y/o plataformas tecnológicas.	Procedimental	Actualizar el procedimiento de desactivación de usuarios actual incluyendo las siguientes mejoras: - Reporte de talento humano debe incluir todas las novedades de nomina (encargos, licencias, incapacidades, vacaciones, situaciones administrativas) - reporte de asuntos contractuales que incluyan todas las novedades de contratación de prestación de servicios (situaciones contractuales) - Enviar reporte de SETIC a SITIC - Solicitar a Talento Humano incluir en el procedimiento "02-P-01 provisión de personal" el reporte semanal de las novedades - Solicitar a la SAC la inclusión del reporte semanal de novedad en el procedimiento "37-G-02 Guía para el ejercicio de las funciones de supervisión y obligaciones de la interventoría"	Sub. Servicios TIC Sub. Infraestructuras TIC Seguridad de la Información Subdirección de Talento Humano Subdirección de asuntos contractuales	31/12/22	Dirección de Informática y Tecnología

V22	Perfiles de usuario de exfuncionarios habilitados en sistemas de información y servicios tecnológicos de la entidad, aún tiempo después de su desvinculación.	Procedimental	Actualizar el procedimiento de desactivación de usuarios actual incluyendo las siguientes mejoras: - Reporte de talento humano debe incluir todas las novedades de nómina (encargos, licencias, incapacidades, vacaciones, situaciones administrativas) - reporte de asuntos contractuales que incluyan todas las novedades de contratación de prestación de servicios (situaciones contractuales) - Enviar reporte de SETIC a SITIC - Solicitar a Talento Humano incluir en el procedimiento "02-P-01 provisión de personal" el reporte semanal de las novedades - Solicitar a la SAC la inclusión del reporte semanal de novedad en el procedimiento "37-G-02 Guía para el ejercicio de las funciones de supervisión y obligaciones de la interventoría"	Sub. Servicios TIC Sub. Infraestructuras TIC Seguridad de la Información Subdirección de Talento Humano Subdirección de asuntos contractuales	31/12/22	Dirección de Informática y Tecnología
V75	Abuso de privilegios por uso de usuarios genéricos.	Procedimental	Configurar seguridad de acceso individual de los administradores de las diferentes plataformas a través de un segundo usuario de red.	Sub. Infraestructuras TIC	30/06/22	Dirección de Informática y Tecnología
V77	Mecanismos de monitoreo, registro y almacenamiento de actividades realizadas durante conexiones remotas, inadecuadas, insuficientes o inexistentes.	Inversión	- Concluir el proceso de contratación de la actualización de la solución. - Implementar herramienta Log Analitic (Azure) en los servidores que controlan la autenticación de los servicios. - Garantizar la inclusión de la solución en el Plan anual de adquisiciones.	Dirección de Informática y Tecnología Sub. Infraestructuras TIC	31/03/22	Dirección de Informática y Tecnología
V77	Mecanismos de monitoreo, registro y almacenamiento de actividades realizadas durante conexiones remotas, inadecuadas, insuficientes o inexistentes.	Mixto	- Revisar la viabilidad de la implementación de una estrategia que permita detectar y/o controlar el número de conexiones remotas inadecuadas, insuficientes o inexistentes. - Establecer el plan de trabajo de acuerdo con el análisis del punto anterior.	Sub. Soluciones TIC Sub. Infraestructuras TIC Seguridad de la Información	31/12/22	Dirección de Informática y Tecnología

V78	Acciones de seguimiento a ingresos y operaciones realizadas a través de los sistemas de información de la Entidad, inadecuados, insuficientes o inexistentes.	Mixto	Se tienen habilitados los logs de todos en los sistemas de información para asegurar la trazabilidad de actividades de usuarios finales y usuarios administradores personalizados. Implementar y procedimentar solución para monitoreo y análisis de logs	Sub. Infraestructura Seguridad de la información	Fase 1: 31/12/2022 Fase 2: 31/12/2023	Dirección de Informática y Tecnología
V80	Mecanismos de control y monitoreo de usuarios genéricos, inadecuados, insuficientes o inexistentes.	Mixto	- Configurar usuarios personalizados de sistema operativo (Linux, Solaris, AIX) con privilegios de root sólo para administradores. - Crear usuarios nombrados para aquellos servicios o plataformas que manejan usuarios genéricos. - Implementar y procedimentar solución para monitoreo y análisis de logs	Sub. Infraestructura Seguridad de la información	Fase 1: 31/12/2022 Fase 2: 31/12/2023	Dirección de Informática y Tecnología
V80	Mecanismos de control y monitoreo de usuarios genéricos, inadecuados, insuficientes o inexistentes.	Inversión	Implementar herramienta para la gestión y centralización de identidades de todos los sistemas de información y servicios de la entidad. Actualizar el procedimiento de desactivación de usuarios actual incluyendo las siguientes mejoras: - Reporte de talento humano debe incluir todas las novedades de nomina (encargos, licencias, incapacidades, vacaciones, situaciones administrativas) - reporte de asuntos contractuales que incluyan todas las novedades de contratación de prestación de servicios (situaciones contractuales) - Enviar reporte de SETIC a SITIC - Solicitar a Talento Humano incluir en el procedimiento "02-P-01 provisión de personal" el reporte semanal de las novedades - Solicitar a la SAC la inclusión del reporte semanal de novedad en el procedimiento "37-G-02 Guía para el ejercicio de las funciones de supervisión y obligaciones de la interventoría"	Dirección de Informática y Tecnología Seguridad de la información	31/10/23	Dirección de Informática y Tecnología

V81	Mecanismos de control y monitoreo de descarga, uso y/o distribución de copias de documentos o de información que por su naturaleza es carácter clasificado y/o reservado, inadecuados, insuficientes o inexistentes.	Inversión	Implementar herramientas o servicios que permitan realizar correlación de eventos, generar bloqueos de extracción o distribución de información acuerdo a las políticas de seguridad configuradas, entrega de informes periódicos de capacidad tecnológica, operación y gestión de incidentes en tiempo real en las siguientes fases: Fase 1: Definición e implementación de solución e incluir en el Plan Anual de Adquisiciones del 2023 Fase 2: Implementar solución	Dirección de Informática y Tecnología Seguridad de la información	Fase 1: 30/06/2022 Fase 2: 31/12/2023	Dirección de Informática y Tecnología
V81	Mecanismos de control y monitoreo de descarga, uso y/o distribución de copias de documentos o de información que por su naturaleza es carácter clasificado y/o reservado, inadecuados, insuficientes o inexistentes.	Mixto	Fase 1: Consolidar la información y definir el mecanismo de etiquetado Fase 2: Etiquetado físico Fase 3: Definición e implementación de mecanismo de etiquetado de información digital e incluir en el Plan Anual de Adquisiciones del 2023 Fase 4: Implementar etiquetado	Subdirección de Gestión Documental Oficina Asesora de Planeación Seguridad de la información Oficina de Análisis y Control de Riesgos Dirección de Informática y Tecnología	Fase 1: 30/06/2022 Fase 2: 31/12/2022 Fase 3: 31/12/2023 Fase 4: 31/12/2024	Dirección de Informática y Tecnología
V81	Mecanismos de control y monitoreo de descarga, uso y/o distribución de copias de documentos o de información que por su naturaleza es carácter clasificado y/o reservado, inadecuados, insuficientes o inexistentes.	Mixto	Solución para restringir gestión y acceso a la información Definir mecanismo o tecnología a adquirir Incluir en el Plan Anual de Adquisiciones del 2023 Realizar Implementación escalonada de la tecnología seleccionada (2023-2024)	Dirección de Informática y Tecnología Seguridad de la información Subdirección Administrativa y Financiera Oficina de Análisis y Control de Riesgos	Fase 1: 31/12/2023 Fase 2: 31/12/2024	Dirección de Informática y Tecnología

V81	Mecanismos de control y monitoreo de descarga, uso y/o distribución de copias de documentos o de información que por su naturaleza es carácter clasificado y/o reservado, inadecuados, insuficientes o inexistentes.	Procedimental	Fase 1: Mesas de trabajo con Talento Humano, seguridad de la información, DIT, OACR y control interno para definir metodología y alcance de la Fase 1 Fase 2: Análisis de alternativas y definición de plan de trabajo para Fase 1.	Dirección de Informática y Tecnología Seguridad de la información Subdirección de TH	Fase 1: 31/10/2022	Dirección de Informática y Tecnología
V86	Autorización de uso de equipos personales sobre los cuales no tiene gobernabilidad la Entidad para trabajo remoto a través de VPN.	Procedimental	- Revisar y documentar lineamientos del control de la norma ISO 27001:2013 control A.11.2.6 a cerca de seguridad en equipos - Implementar lineamiento - Promover el uso de las herramientas de gestión de información de la SDH (office 365)	Dirección de infraestructura TIC Seguridad de la información	31/12/22	Dirección de Informática y Tecnología
V86	Autorización de uso de equipos personales sobre los cuales no tiene gobernabilidad la Entidad para trabajo remoto a través de VPN.	Inversión	Implementar herramientas o servicios que permitan realizar correlación de eventos, generar bloqueos de extracción o distribución de información acuerdo a las políticas de seguridad configuradas, entrega de informes periódicos de capacidad tecnológica, operación y gestión de incidentes en tiempo real en las siguientes fases: Fase 1: Definición e implementación de solución e incluir en el Plan Anual de Adquisiciones del 2023 Fase 2: Implementar solución	Dirección de Informática y Tecnología Seguridad de la información	Fase 1: 30/06/2022 Fase 2: 31/12/2023	Dirección de Informática y Tecnología
V92	La operación de las VPN no esta cubierta por un Servicio de SOC, mediante el cual se entreguen informes periódicos de capacidad tecnológica, operación y gestión de incidentes en tiempo real.	Inversión	Implementar herramientas o servicios que permitan realizar correlación de eventos, generar bloqueos de extracción o distribución de información acuerdo a las políticas de seguridad configuradas, entrega de informes periódicos de capacidad tecnológica, operación y gestión de incidentes en tiempo real en las siguientes fases: Fase 1: Definición e implementación de solución e incluir en el Plan Anual de Adquisiciones del 2023 Fase 2: Implementar solución	Dirección de Informática y Tecnología Seguridad de la información	Fase 1: 30/06/2022 Fase 2: 31/12/2023	Dirección de Informática y Tecnología

V93	Políticas de uso de equipos personales para servicios corporativos inadecuadas, insuficientes o inexistentes.	Procedimental	- Revisar y documentar lineamientos del control de la norma ISO 27001:2013 control A.11.2.6 a cerca de seguridad en equipos - Implementar lineamiento - Promover el uso de las herramientas de gestión de información de la SDH (office 365)	Dirección de infraestructura TIC Seguridad de la información	31/12/22	Dirección de Informática y Tecnología
V93	Políticas de uso de equipos personales para servicios corporativos inadecuadas, insuficientes o inexistentes.	Inversión	Implementar herramientas o servicios que permitan realizar correlación de eventos, generar bloqueos de extracción o distribución de información acuerdo a las políticas de seguridad configuradas, entrega de informes periódicos de capacidad tecnológica, operación y gestión de incidentes en tiempo real en las siguientes fases: Fase 1: Definición e implementación de solución e incluir en el Plan Anual de Adquisiciones del 2023 Fase 2: Implementar solución	Dirección de Informática y Tecnología Seguridad de la información	Fase 1: 30/06/2022 Fase 2: 31/12/2023	Dirección de Informática y Tecnología
V100	Licenciamiento de antivirus sin renovación en estaciones de trabajo.	Procedimental	Hacer solicitud formal a la SAC, para cumplimiento de los tiempos del proceso de contratación.	Sub. Servicios TIC Dirección de informática y Tecnología	30/10/22	Dirección de Informática y Tecnología
V101	Contratos de licenciamiento de antivirus sin compra o renovación al momento del vencimiento de la licencia actual.	Procedimental	Hacer solicitud formal a la SAC, para cumplimiento de los tiempos del proceso de contratación.	Sub. Servicios TIC Dirección de informática y Tecnología	30/10/22	Dirección de Informática y Tecnología
V102	Envió de agentes de antivirus no extensivo a todos los equipos de la Entidad.	Procedimental	Generar documento para soportar la instalación, puesta en funcionamiento y seguimiento a la operación del antivirus que incluya: - Instalación punto a punto de los computadores nuevos. - Actualizar el agente semanalmente en todos los computadores de la entidad.	Dirección de Informática y Tecnología	30/06/22	Dirección de Informática y Tecnología

V103	Denegación de acceso a actualización de firmas de antivirus por parte del proveedor.	Procedimental	Hacer solicitud formal a la SAC, para cumplimiento de los tiempos del proceso de contratación.	Sub. Servicios TIC Dirección de informática y Tecnología	30/10/22	Dirección de Informática y Tecnología
V105	Desarticulación de información entre bases de usuarios administrada por Talento Humano, Informática y Tecnología y Asuntos Contractuales y las dependencias funcionales que tienen aplicativos a cargo.	Procedimental	Implementar herramienta para la gestión y centralización de identidades de todos los sistemas de información y servicios de la entidad. Actualizar el procedimiento de desactivación de usuarios actual incluyendo las siguientes mejoras: - Reporte de talento humano debe incluir todas las novedades de nomina (encargos, licencias, incapacidades, vacaciones, situaciones administrativas) - reporte de asuntos contractuales que incluyan todas las novedades de contratación de prestación de servicios (situaciones contractuales) - Enviar reporte de SETIC a SITIC - Solicitar a Talento Humano incluir en el procedimiento "02-P-01 provisión de personal" el reporte semanal de las novedades - Solicitar a la SAC la inclusión del reporte semanal de novedad en el procedimiento "37-G-02 Guía para el ejercicio de las funciones de supervisión y obligaciones de la interventoría"	Sub. Servicios TIC Sub. Infraestructuras TIC Seguridad de la Información Subdirección de Talento Humano Subdirección de asuntos contractuales	31/12/22	Dirección de Informática y Tecnología

V109	Los logotipos utilizados para comunicaciones oficiales de la entidad están disponibles para cualquier funcionario o contratista que tenga acceso a la intranet, sin restricción de configuración, copia o impresión.	Inversión	- Revisar todos los procesos de la SDH que usan la herramienta CRM, con el fin de establecer si manejan algún tipo de validación. - Verificar como funciona actualmente en BogData el envío de los Actos Oficiales de Impuestos, que son enviados por notificaciones y que tienen afectación de dinero y si manejan código QR para verificación de validez de documento, - Definir el plan de trabajo para implementación de seguridad aplicada a las comunicaciones y notificaciones que lo requiera dependiendo del módulo de Bogdata al que correspondan. - Ajuste de documentos del SGC.	Sub. Soluciones TIC Seguridad de la Información Gerencia proyecto BogData	31/12/22	Dirección de Informática y Tecnología